

UNIVERSITÀ
DEGLI STUDI
DI PADOVA



UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

LAUREA TRIENNALE IN

INGEGNERIA DELL'INFORMAZIONE

Gaussian Boson Sampling

Correlatore:

PROF. GIUSEPPE PINO VALLONE

Studente:

MARCO POLO

MATRICOLA 1163996

ANNO ACCADEMICO 2022/2023

DATA 21/7/2023

*A person who never made a
mistake never tried anything new.*

Albert Einstein

Indice

Introduzione	2
1 Il computer quantistico	3
1.1 Principio di sovrapposizione	3
1.1.1 Il gatto di Schrödinger	5
1.2 Entanglement Quantistico	6
1.3 Qubit	7
1.3.1 Tipologie di qubit	9
1.3.2 I bosoni	10
1.3.3 Fotonica Integrata	11
1.3.4 I fotoni come qubit	12
2 Gaussian Boson Sampling	14
2.1 Boson Sampling	14
2.1.1 Preparazione dello stato di input	14
2.1.1.1 Modi di un sistema quantistico	15
2.1.1.2 Stati di un sistema quantistico	16
2.1.1.3 Base di Fock	17
2.1.2 Rete ottica	17
2.1.3 Interferenza e misurazione	19
2.1.4 Distribuzione di probabilità	19
2.1.4.1 Scattering matrix o Unitary matrix	20
2.1.4.2 Permanente della scattering matrix	21
2.2 Gaussian Boson Sampling (GBS)	24
2.2.1 Stati Gaussiani	24
2.2.2 Squeezed light	25
2.2.3 Hafniano della Scattering matrix	27
2.3 Obiettivi di GBS	28
2.3.1 Teorema esteso di Church-Turing	28
3 Il processore quantico fotonico Borealis	29
3.1 Overview del Progetto	29
3.1.1 Time Domain Multiplexing (TDM)	30
3.1.2 Cluster States	31
3.2 Circuito ottico	32

3.3	Analisi dell'esperimento	34
3.3.1	Esecuzione dell'esperimento di campionamento con un basso numero di fotoni e modalità	34
3.3.2	Esecuzione dell'esperimento di campionamento con un numero moderato di fotoni e modalità	36
3.3.3	Esecuzione dell'esperimento di campionamento con un numero elevato di fotoni e modalità	37
3.4	raggiungimento del vantaggio quantico	40
	Conclusione	41
	Bibliografia e Sitografia	43

Introduzione

Il Quantum Computing è un argomento ormai ben consolidato all'interno della teoria dell'informazione e ad oggi le sue applicazioni abbracciano moltissimi rami dell'informatica. I benefici e le capacità offerte dai sistemi quantistici rispetto ai sistemi classici per determinati tipi di calcoli, o attività di elaborazione delle informazioni, derivano dalle proprietà e dai principi unici della meccanica quantistica che consentono a tale sistemi di eseguire computazioni estremamente complesse in un periodo di tempo ragionevolmente limitato. La notevole differenza tra i sistemi classici e quelli quantistici nello svolgimento di determinati compiti ha portato nel 2012 alla teorizzazione della così detta Supremazia Quantistica (*Quantum Supremacy*).

Il concetto di supremazia quantistica è stato proposto per la prima volta da John Preskill nel 2012 [1]. Questo suggerisce che un computer quantistico può superare i computer classici nell'esecuzione di un compito computazionale ben definito, rappresentando una dimostrazione della potenziale superiorità computazionale dei sistemi quantistici rispetto alle controparti classiche nello svolgimento di determinate operazioni. Tale teoria è stata poi più volte dimostrata nel corso degli anni a venire attraverso la realizzazione di sistemi di calcolo quantistico estremamente efficienti.

È importante notare però che: sebbene il vantaggio quantistico esista, e sia ad oggi ben consolidato, esso non sia universale per tutte le attività computazionali. Ci sono infatti problemi e compiti per i quali i computer classici rimangono efficienti ed efficaci. Inoltre: le implementazioni pratiche dei computer quantistici affrontano sfide come il rumore, la correzione degli errori e la scalabilità. Nonostante ciò, la ricerca dei vantaggi quantistici continua a guidare gli studi nel campo, con l'obiettivo di sfruttare le proprietà uniche dei sistemi quantistici per risolvere i problemi del mondo reale in modo più efficiente ed efficace.

In questa stesura si vuole però approfondire come la risoluzione di un problema estremamente complesso come il *Gaussian Boson Sampling (GBS)*, permetta ad un compilatore quantistico programmabile, che sfrutta tecnologia fotonica, di raggiungere il vantaggio quantistico, settando il limite su ciò che un computer classico sia in grado di risolvere in un periodo di tempo quantificabile.

Capitolo 1

Il computer quantistico

Prima di addentrarci nello specifico all'interno di questo argomento è bene fare un passo indietro e introdurre i concetti principali legati alla teoria dell'informazione quantistica. Iniziamo con il considerare il funzionamento di un calcolatore classico: esso, infatti, rispetta il modello di *macchina di Turing*[2] (teorizzato ormai oltre ottant'anni fa), attraverso cui l'informazione è rappresentata da stringhe di "0" e "1", tali unità fondamentali prendono il nome di BIT (*Binary Digit*). Questa combinazione di BIT rappresenta uno stato ben definito dell'informazione da elaborare, rendendo i sistemi di elaborazione classici sistemi così detti sequenziali.

A differenza dei sistemi classici però, quelli quantistici possono esistere in stati di sovrapposizione che rappresentano a loro volta una combinazione di stati diversi contemporaneamente; ciò consente il calcolo parallelo, poiché gli algoritmi quantistici possono operare su più input contemporaneamente. Un'altra peculiarità di questi sistemi è l'*Entanglement* (1.2) quantistico: fenomeno in cui gli stati di più particelle vengono correlati in modo tale che il comportamento di una particella sia istantaneamente collegato al comportamento di un'altra, indipendentemente dalla loro separazione spaziale.[3]

1.1 Principio di sovrapposizione

Nella fisica classica ciò che ci circonda è descritto da proprietà ben definite, il che ci limita all'esistenza in un solo stato alla volta. Tuttavia, nella meccanica quantistica, particelle e sistemi possono esibire un comportamento ondulatorio che permette loro di trovarsi in una sovrapposizione di più stati contemporaneamente, ciascuno con una specifica ampiezza di probabilità, tale comportamento dei sistemi quantistici è descritto dal *principio di sovrapposizione*.

Questo in particolare afferma che: se un sistema quantistico si trova in uno stato che può essere espresso come una combinazione lineare di altri stati, allora il sistema può esistere anche in una sovrapposizione di essi.[4]

Per descrivere al meglio il principio di sovrapposizione partiamo però analizzando un caso classico, ovvero il lancio di una moneta.[5] Questo sistema produrrà come

risultato due stati ben distinti, quello in cui osserveremo la faccia riportante **Testa (T)** o quello in cui la faccia osservata sarà **Croce (C)**, entrambi caratterizzati dalla stessa probabilità.

$$P(T) = \frac{1}{2} \quad P(C) = \frac{1}{2} \quad (1.1)$$

Per quanto riguarda il caso quantistico, matematicamente, il principio di sovrapposizione è rappresentato da una funzione d'onda (indicata con la lettera Ψ) anche detta *vettore di stato*, che descrive lo stato quantistico di un sistema. La funzione d'onda assegna un'ampiezza di probabilità complessa a ogni possibile stato, il cui modulo al quadrato ne fornisce la relativa densità di probabilità.

Ne è una prova evidente l'esperimento della *doppia fenditura*, in cui un elettrone viene lanciato addosso a due fenditure.[6][7] Le casistiche (che da ora in poi chiameremo *modalità*) rilevabili dall'esperimento prevedono che l'elettrone attraversi la **Fenditura 1 (F1)**, oppure attraversi la **Fenditura 2 (F2)**. Le probabilità relative alle due modalità saranno dunque descritte da due funzioni d'onda ben distinte, rispettivamente Ψ_1 e Ψ_2 , da cui si ricava:

$$\Psi_{tot} = \Psi_1 + \Psi_2 \quad (1.2)$$

con relativa densità di probabilità:

$$P_{tot}(r, t) = |\Psi_{tot}|^2 \quad (1.3)$$

$P_{tot}(\mathbf{r}, t)$ fornisce la descrizione probabilistica di rilevare l'elettrone al di fuori di una o dell'altra fenditura.

Per la proprietà matematica di linearità del sistema, date due funzioni d'onda Ψ_1 e Ψ_2 sarà allora verificata la relazione:

$$\Psi_{tot} = \alpha_1 \Psi_1 + \alpha_2 \Psi_2 \quad (1.4)$$

Con α_1 e α_2 costanti arbitrarie, e sarà anch'essa soluzione del sistema. Ciò comporta che l'elettrone all'uscita dalle fenditure può essere descritto dalla funzione d'onda Ψ_1 (che indica il passaggio dalla **Fenditura 1 (F1)**), può essere descritto dalla funzione d'onda Ψ_2 (che indica il passaggio dalla **Fenditura 2 (F2)**). Oppure può essere descritto dalla funzione d'onda Ψ_{tot} che indica il passaggio sia attraverso la **Fenditura 1 (F1)** sia dalla **Fenditura 2 (F2)**.

Volendo dare una interpretazione fisica molto semplificata a livello macroscopico del risultato appena descritto, possiamo utilizzare come esempio l'onda generata dalla corda tesa di una chitarra. Tale corda potrà vibrare alla frequenza \mathbf{f}_1 oppure \mathbf{f}_2 . E' possibile quindi sommarle, $\mathbf{f}_{tot} = \mathbf{f}_1 + \mathbf{f}_2$ e dunque far vibrare la corda alla frequenza risultante, anch'essa soluzione del sistema.

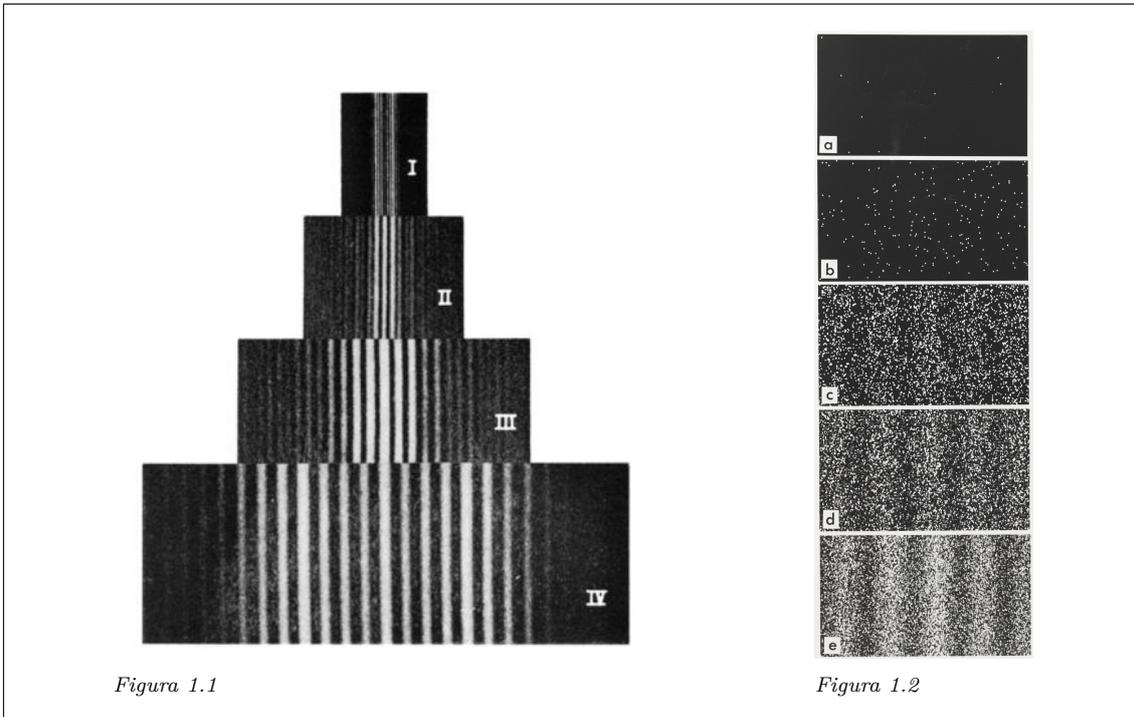


Figura 1.1

Figura 1.2

Figura 1.1: Figura di interferenza con numero di elettroni progressivamente variabile.

Figura 1.2: Esperimento della doppia fenditura effettuato con elettroni singoli.

Viene spontaneo allora chiedersi: come è possibile effettuare delle misurazioni su tale tipologia di sistema? Ebbene quando esse vengono eseguite su di un sistema quantistico in sovrapposizione, la funzione d'onda "collassa" in uno dei possibili stati e il sistema viene osservato in quello specifico stato con relativa probabilità data da $P_{\text{tot}}(\mathbf{r}, t)$. [8]

1.1.1 Il gatto di Schrödinger

Per cercare di dare una interpretazione del principio di sovrapposizione possiamo considerare l'esperimento del *gatto di Schrödinger*, teorizzato dal fisico e matematico Austro-Ungarico *Erwin Schrödinger* nel 1935. [9] Si tratta del esempio ideale per cercare di applicare ad un sistema macroscopico la sovrapposizione delle funzioni d'onda, osservabili però solo a livello microscopico.

L'esperimento consiste nel rinchiudere al interno di un contenitore chiuso un gatto e una fialetta contenente del veleno che si romperà in un momento casuale. Ciò che determinerà la rottura della fialetta di veleno è una minuscola quantità di sostanza radioattiva posizionata sul sensore di un rivelatore Geiger. La quantità di quest'ultima sarà così irrisoria che nel corso di un'ora potrebbe decadere uno solo degli atomi che la compone e con la stessa probabilità anche nessuno. Nel caso in cui uno dei suoi atomi decada, il rivelatore Geiger lo rileverebbe rompendo la fialetta

di veleno e uccidendo il gatto.

Dopo aver lasciato indisturbato questo intero sistema per un'ora, ovvero il tempo minimo per l'eventuale decadimento di un atomo, il gatto potrebbe essere ancora vivo (se nessun atomo della sostanza radioattiva fosse decaduto) o morto (in caso contrario). Volendo però studiarle nel dettaglio, le funzioni d'onda che descrivono il sistema completo, esprimeranno questo fatto per mezzo della combinazione di due termini che si riferiscono al gatto vivo e al gatto morto. Dopo un'ora il sistema potrà quindi trovarsi nella sovrapposizione di due stati e solamente aprendo il contenitore si verificherà il collasso della funzione d'onda, che precipiterà in uno stato oppure nel altro. L'assurdo (dovuto al fatto che stiamo considerando un numero troppo elevato di atomi) dunque si verifica esattamente in questo momento: infatti è come se, prima che io apra il contenitore, il gatto sia contemporaneamente sia vivo che morto e solamente nel momento in cui lo aprirò esso decida in quale dei due stati trovarsi.

1.2 Entanglement Quantistico

L'*entanglement quantistico* o *correlazione quantistica* è un concetto fondamentale della meccanica quantistica che descrive la forte correlazione e interdipendenza tra le particelle anche se fisicamente separate. Quando più particelle sono correlate (in inglese "*entangled*"), i loro stati quantistici risultano collegati, in questo modo lo stato di una particella non può essere descritto indipendentemente dallo stato delle altre particelle nel sistema. Ad esempio: se due particelle vengono preparate in una sovrapposizione di stati e quindi lasciate interagire, i loro stati possono diventare correlati ma, tali correlazioni, non possono essere spiegate dalla fisica classica. Ciò comporta che il concetto di entanglement sfidi le intuizioni classiche che abbiamo di ciò che ci circonda, in quanto dimostra come il mondo quantistico operi in modo diverso da quello in cui viviamo tutti i giorni.[10]

L'aspetto intrigante dell'entanglement inoltre è come gli stati delle particelle correlate siano intrecciati in modo tale che la misurazione dello stato di una particella determini istantaneamente lo stato dell'altra, indipendentemente dalla distanza fisica che intercorre tra loro. Questo fenomeno prende spesso il nome di *spaventosa azione a distanza*, poiché gli effetti della misurazione sembrano verificarsi più velocemente della velocità della luce.

L'entanglement svolge un ruolo centrale nei fondamenti della meccanica quantistica e della scienza dell'informazione quantistica; è inoltre stato ampiamente studiato e verificato attraverso diversi esperimenti: in particolare tramite la violazione della *disuguaglianza di Bell*. Il termine teoricamente potrebbe indicare una qualsiasi

dell'insieme di disuguaglianze, ma in pratica, negli esperimenti reali, ci si riferisce alle disuguaglianze *CHSH* e *CH74* e non a quella originale ricavata da Bell. Esse pongono restrizioni sui risultati statistici di esperimenti su coppie di particelle che hanno preso parte a un'interazione e poi separate. Nel 2019 attraverso misurazioni in laboratorio del fenomeno dell'Entanglement è stato possibile immortalarlo. [11]

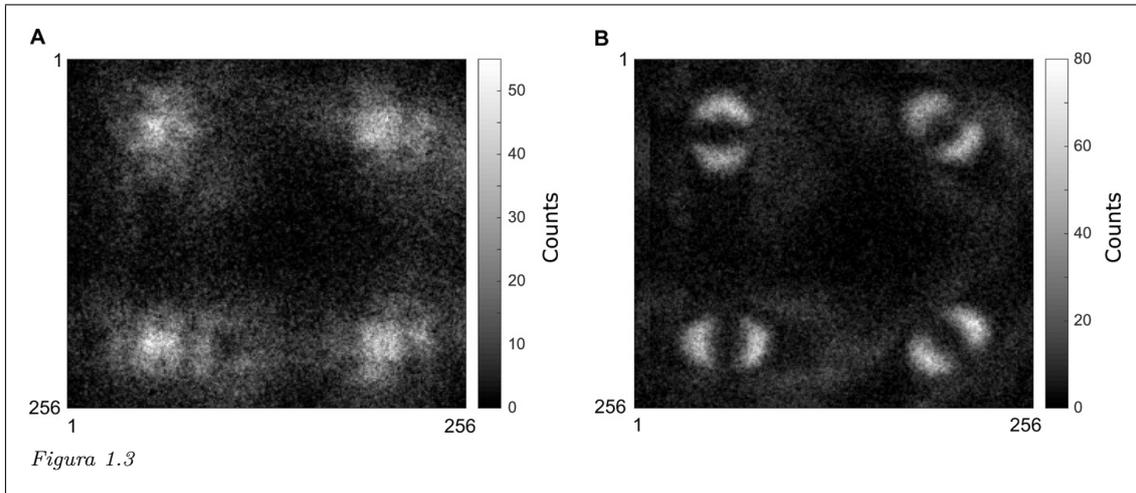


Figura 1.3: Immagine full frame che registra la violazione della disuguaglianza di Bell e implementa la scansione del cerchio di fase.

1.3 Qubit

Ora che abbiamo ben chiaro come il principio di sovrapposizione abbia profonde implicazioni per il calcolo quantistico e l'elaborazione delle informazioni quantistiche, possiamo introdurre l'unità fondamentale che costituisce i computer quantistici, ovvero il **QUBIT** (*Quantum BIT*). Tale unità fondamentale, a differenza dei classici BIT, che possono rappresentare esclusivamente il valore "0" o "1", può rappresentare lo **STATO QUANTISTICO 0**, indicato con $|0\rangle$, oppure lo **STATO QUANTISTICO 1**, indicato con $|1\rangle$, e grazie al principio di sovrapposizione, anche lo stato che si trova tra i due precedenti, chiamato **SOVRAPPOSIZIONE COERENTE DI STATI** o **SUPERPOSIZIONE** e rappresentato attraverso la combinazione lineare:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.5}$$

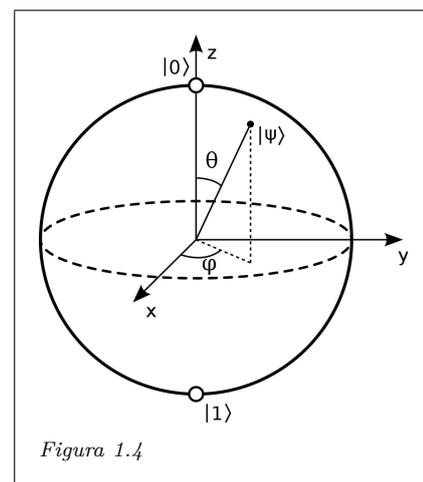


Figura 1.4: Rappresentazione di un qubit attraverso la sfera di Bloch

Con α e β coefficienti complessi detti ampiezze di probabilità.

Ovviamente non è possibile leggere direttamente il valore trasportato da un qubit, ben più agevole è invece verificare con che valore di probabilità esso si trovi in uno stato piuttosto che in un altro. Possiamo definire dunque:

$$\begin{aligned} |\alpha|^2 &= P(|0\rangle) \\ |\beta|^2 &= P(|1\rangle) \end{aligned} \quad (1.6)$$

Con:

$$P(|0\rangle) + P(|1\rangle) = |\alpha|^2 + |\beta|^2 \leq 1 \quad (1.7)$$

Dunque grazie al principio di sovrapposizione un qubit può esistere in uno stato continuo compreso tra $|0\rangle$ o $|1\rangle$ fino a che non viene osservato. Una volta osservato infatti esso decadrà o in uno o nel altro stato.

Per rendere più chiaro di cosa stiamo parlando diamo dei valori ai coefficienti e cerchiamo di esprimerne la probabilità. Assumendo:

$$\alpha = \frac{1}{\sqrt{2}} \quad e \quad \beta = \frac{1}{\sqrt{2}} \quad (1.8)$$

Vale:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (1.9)$$

E dunque:

$$|\alpha|^2 = \frac{1}{2} \quad e \quad |\beta|^2 = \frac{1}{2} \quad (1.10)$$

Si conclude dunque che fino all'osservazione dello stato del qubit, esso potrà trovarsi con lo stesso valore di probabilità $P(|0\rangle) = P(|1\rangle) = \frac{1}{2}$, nello **STATO 0** o nello **STATO 1**, ed è proprio questo lo stato di **SOVRAPPOSIZIONE COERENTE DI STATI** o **SUPERPOSIZIONE**, indicato in (1.9)

Il principio di sovrapposizione intrinsecamente legato ai qubit consente dunque il calcolo parallelo e l'elaborazione contemporanea di più sequenze di dati.[12]

I qubit possono inoltre essere combinati tra loro attraverso porte quantistiche (*quantum gates*), che possono modificare le ampiezze di probabilità e la correlazione tra i qubit. Il risultato di tale combinazione è uno stato quantico composto che rappresenta un sistema estremamente correlato.

Ecco allora che l'entanglement quantistico gioca un ruolo cruciale nell'elaborazione dell'informazione quantistica, in quanto consente la creazione di stati altamente correlati indipendentemente dalla separazione spaziale dei singoli qubit.[13]

Quella che ho precedentemente illustrato è solo una trattazione generale e semplificata della teoria alla base dei qubit, ci sarebbero infatti molti altri aspetti da considerare

legati soprattutto ai fenomeni di distorsione dell'informazione. Uno tra tutti è il fenomeno della *decoerenza*, che si riferisce alla perdita di informazioni quantistiche dovuta alle interazioni con l'ambiente. Tali fenomeni e relative tecniche di rilevamento e correzione richiederebbero una trattazione separata e del tutto superflua ai fini della comprensione della stesura.

Più interessante è la definizione di alcune tecnologie per la realizzazione dei qubit.

1.3.1 Tipologie di qubit

Esistono varie tecnologie utilizzate per la realizzazione dei qubit, ciascuno con i propri vantaggi e sfide. Anche in questo caso la trattazione richiederebbe riflessioni dettagliate su ognuna delle tecnologie che andrò a citare di seguito, ma ai fini della comprensione della stesura, andrò ad approfondire esclusivamente quella legata ai fotoni:

- **Circuiti superconduttori:** Realizzati attraverso circuiti elettrici superconduttori, questi sono una delle tecnologie più promettenti non che più utilizzate per la realizzazione di un computer quantistico scalabile e resistenti agli errori.
- **Ioni intrappolati:** Gli ioni vengono intrappolati utilizzando campi elettromagnetici e in seguito manipolati e misurati utilizzando raggi laser. I livelli di energia interna agli ioni ne determinano gli stati dei qubit. I qubit ionici intrappolati hanno dimostrato lunghi tempi di coerenza e operazioni ad alta fedeltà.[14]
- **Punti quantici:** I punti quantici sono minuscole strutture semiconduttrici che possono confinare un piccolo numero di elettroni. Gli stati di spin o carica degli elettroni confinati sono usati come qubit. I punti quantici possono essere controllati e misurati utilizzando tensioni elettriche e campi magnetici, inoltre essi presentano il potenziale per l'integrazione con le tecnologie dei semiconduttori esistenti.[15]
- **Qubit topologici:** Una innovativa tecnica di realizzazione dei qubit è rappresentata dai qubit topologici che si basano sul concetto di stati topologici della materia. Alcuni stati "esotici" della materia, come i *fermioni di Majorana*, sono usati per codificare e manipolare informazioni quantistiche. Questi qubit hanno proprietà intrinseche di protezione dagli errori e vengono studiati per la loro robustezza contro il rumore e la decoerenza.[16]
- **Risonanza magnetica nucleare (NMR):** i qubit basati su **NMR** utilizzano gli spin dei nuclei atomici come stati quantici associati ai qubit. Le tecniche **NMR** applicano campi magnetici e impulsi a radiofrequenza per manipolare e misurare gli spin nucleari. Sebbene i qubit **NMR** siano stati dimostrati

sperimentalmente, devono affrontare sfide in termini di scalabilità e precisione, prima di poter essere fisicamente utilizzati.[17]

- **Diamond Vacancy Centers:** Alcuni difetti nel diamante, come i *centri di azoto vacante* (**NV**), possono essere usati come qubit. Gli stati di spin elettronico dei centri **NV** possono essere controllati e misurati utilizzando campi magnetici e luce laser. I qubit a base di diamante hanno mostrato il potenziale per il rilevamento quantistico e le applicazioni di comunicazione quantistica.[18]

Queste sono le tecnologie ad oggi più utilizzate in campo quantistico per la realizzazione di qubit, ma lo studio per svilupparne di nuove, al fine di migliorare le prestazioni dei qubit, prosegue in maniera serrata. La scelta della tecnologia dipende da fattori quali scalabilità, tempi di coerenza, controllabilità e compatibilità con le tecniche di correzione degli errori.

Resta inoltre un'ultima rilevante tecnica di realizzazione di qubit che prevede l'utilizzo di **fotoni** (particelle di luce): essa infatti sarà di fondamentale importanza per la comprensione della stesura ed è per questo motivo che verrà trattata maggiormente nel dettaglio.

1.3.2 I bosoni

Prima di esaminare l'utilizzo di fotoni come qubit, è bene introdurre alcune nozioni fondamentali legate alla fisica delle particelle elementari.

Nella fisica delle particelle, quelle elementari sono classificate in due grandi categorie: *fermioni* e *bosoni*, in base alle loro proprietà quantomeccaniche.

Definizione 1 (Bosone). Un bosone è un tipo di particella elementare che appartiene a una classe di particelle note come *portatori di forza* o *bosoni di gauge*; essi hanno valori interi di *spin*, proprietà intrinseca delle particelle che ne caratterizza il momento angolare e ne determina il comportamento in rotazione.

I bosoni inoltre seguono un insieme distinto di regole della meccanica quantistica chiamate statistiche di Bose-Einstein, che differiscono dalle regole che governano i fermioni, note come statistiche di Fermi-Dirac.

I bosoni svolgono un ruolo cruciale nelle interazioni fondamentali in natura, eccone i principali esempi:

- **Bosoni W e Z:** I bosoni W e Z sono responsabili della mediazione della forza nucleare debole, che governa processi come il decadimento radioattivo. Hanno uno spin pari a 1 e sono particelle relativamente massicce[19]

- **Gluone:** I gluoni sono le particelle che mediano la forza nucleare forte, che tiene insieme i nuclei atomici. Hanno uno spin pari a 1 e portano la carica di valore associata alla forza forte.[19]
- **Bosone di Higgs:** Il bosone di Higgs è una particella scoperta di recente, associata al campo di Higgs, che dà massa ad altre particelle. Ha uno spin pari a 0 ed è relativamente pesante rispetto ad altre particelle elementari.[19]
- **Fotone:** Il fotone è la particella fondamentale della luce e il portatore della forza elettromagnetica. I fotoni hanno spin pari a 1 e non hanno massa.[19]

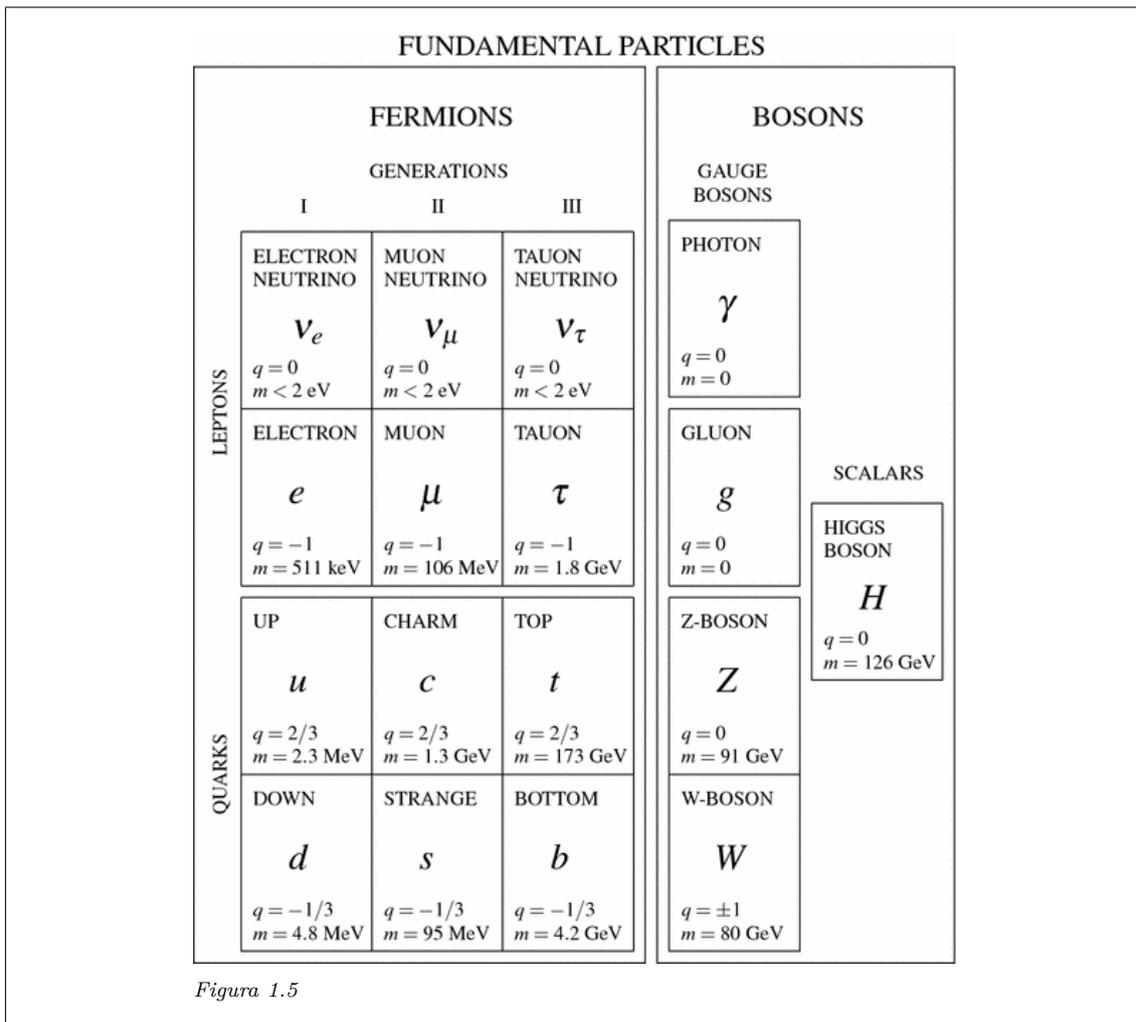


Figura 1.5: Modello standard delle particelle elementari

1.3.3 Fotonica Integrata

E' bene introdurre anche la branca della fisica che studia gli effetti e le implicazioni dell'utilizzo di fotoni sfruttandone il loro comportamento. La *fotonica* è la scienza che studia l'interazione della luce con la materia, dalla scala atomica a quella astronomica, dalla fotonica si è sviluppato il laser, le comunicazioni in fibra ottica e moltissimi

altri sensori che pervadono la tecnologia odierna. Dall'unione della fotonica con le nanotecnologie nasce poi la *fotonica integrata*, una nuova branca della fisica che permette di manipolare la luce in strutture microscopiche, raggiungendo intensità del campo magnetico altrimenti impensabili in sistemi convenzionali. Il risultato è la possibilità di osservare fenomeni fisici nuovi, che coinvolgono i singoli quanti della radiazione elettromagnetica, ovvero i fotoni, che in questo regime dominano le leggi della meccanica quantistica. Manipolando dunque la luce a livello dei singoli fotoni è possibile sfruttarne le proprietà uniche per utilizzarli come portatori di informazione quantistica per realizzare computer dalle prestazioni a dir poco strabilianti.

Rallentando infatti i fotoni è possibile realizzare una stranissima e nuova forma di luce, detta, luce compressa (*squeezed light* (2.2.2)). Proprio questa recente creazione è alla base del funzionamento del processore quantico fotonico di cui parleremo ampiamente più avanti nella discussione, e che ha portato alla risoluzione di problemi finora al di fuori della portata dei più potenti supercomputer.

1.3.4 I fotoni come qubit

Il fotone è tra le particelle più interessanti studiate dalla fisica particellare, esso ha vita infinita, può essere creato e distrutto dall'interazione con altre particelle, ma non può decadere spontaneamente. Pur non avendo massa è influenzato dalla gravità e possiede energia; nel vuoto si muove alla velocità della luce, mentre nella materia si comporta in modo diverso e la sua velocità può scendere al di sotto di quella della luce. *Bohr* ipotizzò che un atomo possa emettere un'onda elettromagnetica (o radiazione) solo quando un elettrone si trasferisse da un'orbita con energia maggiore (\mathbf{E}_i) a un'orbita con energia minore (\mathbf{E}_f). L'energia della radiazione elettromagnetica emessa dall'atomo non può avere qualsiasi valore, ma solo quantità discrete, dette quanti di energia, ovvero, i fotoni.

Essi possono essere manipolati e controllati per codificare le informazioni in relativi stati quantistici, rendendoli candidati idonei per i qubit; sono relativamente robusti contro la decoerenza causata dalle interazioni con l'ambiente, il che li rende buoni candidati per la comunicazione a lunga distanza e la crittografia quantistica mostra inoltre una bassa interazione tra loro, consentendo la creazione di stati correlati, tra qubit distanti.

Esistono diversi approcci per codificare le informazioni quantistiche nei fotoni: il metodo più utilizzato consiste nell'usare la polarizzazione del fotone per rappresentare gli stati dei qubit. Lo stato di polarizzazione di un fotone può essere **polarizzato orizzontalmente** ($|0\rangle$) o **polarizzato verticalmente** ($|1\rangle$), o una **sovrapposizione di questi stati** ($|\Psi\rangle$).[20]

Tuttavia, l'utilizzo dei fotoni nel campo dell'informatica quantistica ha richiesto la

risoluzione di grosse problematiche come la loro mancanza di interazioni naturali, che può rendere difficile realizzare determinate porte quantistiche. Inoltre i fotoni sono tipicamente di natura probabilistica e spesso sono necessarie misurazioni per estrarre informazioni da essi, il che può risultare difficile per alcuni tipi di algoritmi quantistici.

Capitolo 2

Gaussian Boson Sampling

2.1 Boson Sampling

Il *Boson Sampling* è un problema computazionale che implica la manipolazione e la misurazione di fotoni per eseguire calcoli specifici. Esso ha attirato l'attenzione nel campo dell'informatica quantistica in quanto mette in luce i potenziali vantaggi dei sistemi quantistici rispetto ai computer classici. A differenza di altre attività di calcolo quantistico che richiedono il controllo universale sul sistema, il Boson Sampling può essere implementato sulle attuali piattaforme sperimentali fotoniche, rendendolo una strada pratica e promettente per esplorare i vantaggi quantistici. Nel Boson Sampling, l'input del sistema è un insieme di fotoni indistinguibili che vengono iniettati in una complessa rete di sfasatori e divisori di fascio; i fotoni quindi escono dalla rete e vengono misurati in specifiche porte di uscita.

2.1.1 Preparazione dello stato di input

Iniziamo la trattazione considerando l'input del sistema che prevede l'immissione di singoli fotoni in diversi canali di ingresso del circuito. I fotoni vengono iniettati in modo tale da interferire tra loro e possono essere preparati in una configurazione specifica, ad esempio utilizzando un laser o altre sorgenti.

La configurazione specifica degli stati di input dipende dall'esperimento desiderato e dal problema da risolvere, inoltre la scelta di tali stati può influenzare la complessità e l'output dell'esperimento. Diverse configurazioni di input possono portare a diversi modelli di interferenza e probabilità di output, influenzando le proprietà computazionali del sistema.

Prima di scendere nel dettaglio dell'analisi degli stati di input nel campo del Boson Sampling conviene prendere familiarità con il concetto di *stato*, per come esso viene inteso all'interno della teoria dell'informazione quantistica; per farlo, partiremo dal concetto di *modo*.

2.1.1.1 Modi di un sistema quantistico

Prima di introdurre il concetto di modi all'interno di un sistema quantistico è bene avere un'idea ben chiara della sua controparte classica. Nell'informatica classica, le modalità computazionali si riferiscono in genere a diversi modi o configurazioni in cui un computer o un sistema informatico può operare.

Alcuni esempi di modalità computazionali nel calcolo classico sono: -le *modalità operative*, che definiscono il modo in cui il sistema opera e interagisce con l'utente; -le *modalità di esecuzione* prevalentemente legate all'hardware, possono influire sul comportamento e sui livelli di privilegio delle istruzioni software; -le *modalità di alimentazione*, atte ad ottimizzare il consumo energetico.

Mentre per le architetture classiche il concetto di modalità è strettamente legato alle caratteristiche di realizzazione dell'hardware, nell'informazione quantistica il termine modalità si riferisce tipicamente ai diversi gradi di libertà o variabili indipendenti associate a un sistema quantistico. Queste modalità possono essere quantità fisiche, come la posizione o la quantità di moto di una particella, o proprietà astratte, come la polarizzazione o il livello di energia di un fotone. Ai fini della comprensione dei paragrafi successivi possiamo limitarci alla trattazione di soli 2 modi:

- **Modalità spaziali:** Nella fotonica integrata, i fotoni possono essere descritti in termini di modalità spaziali. Queste modalità rappresentano diversi schemi spaziali o distribuzioni di valori di ampiezza del campo elettrico del fotone.
- **Modalità di polarizzazione:** Un'altra descrizione dei fotoni introdotta nella fotonica integrata, è attraverso le modalità di polarizzazione, in cui lo stato di polarizzazione di un fotone si riferisce all'orientamento dell'oscillazione del campo elettrico.

Per completezza, è bene citare comunque anche altre modalità comunemente utilizzate nella trattazione di sistemi di calcolo quantistico, quali:

-*Modalità di spin*, in cui le particelle dotate di spin, come gli elettroni o alcuni tipi di atomi, associano all'orientamento del loro momento angolare di spin diverse modalità. Tali stati di spin possono essere usati per codificare informazioni in un qubit, che può essere definito utilizzando due stati di rotazione: "su" e "giù" lungo un asse specifico.

-*Modi temporali*: in alcuni sistemi quantistici, come ioni intrappolati o circuiti superconduttori, il tempo può essere considerato come un modo. Questi sistemi possono essere manipolati controllando l'evoluzione dei loro stati quantistici nel tempo. Le porte e le operazioni quantistiche dipendenti dal tempo possono essere realizzate secondo una serie di vincoli legati a queste modalità.

-*Modalità di frequenza*: spesso utilizzata nei sistemi quantistici che sfruttano gli ioni come portatori di informazione, i livelli di energia possono essere utilizzati per

definire le modalità di frequenza.

Ogni modo corrisponde a uno specifico livello di energia o frequenza associata al sistema.

I modi svolgono dunque un ruolo cruciale nell'elaborazione delle informazioni quantistiche in quanto la comprensione e il controllo delle diverse modalità di un sistema ne forniscono la base per la codifica e la manipolazione degli stati.

2.1.1.2 Stati di un sistema quantistico

Abbiamo appena visto come i modi rappresentino le diverse configurazioni o gradi di libertà di un sistema, mentre lo stato fornisce una distribuzione di probabilità per i risultati di ogni possibile misurazione su un sistema. Esiste dunque un'interconnessione tra i due concetti, in particolare i modi forniscono una base per costruire gli stati che descriveranno probabilisticamente lo stato quantistico del sistema.

Gli stati quantistici sono tipicamente rappresentati da oggetti matematici chiamati *vettori di stato*, che contengono informazioni sulle ampiezze di probabilità associate a diversi possibili risultati delle misurazioni. Tali vettori appartengono a uno spazio vettoriale complesso noto come *spazio di Hilbert*. Lo spazio di Hilbert descrive tutti i possibili stati che il sistema può occupare.

Per aiutare la comprensione del lettore possiamo descrivere una situazione comune nel calcolo quantistico, in cui i qubit rappresentano una modalità o grado di libertà. Lo stato quantistico dell'intero sistema, composto da più qubit, è descritto dal prodotto tensoriale dei singoli stati dei qubit, il cui risultato può dunque essere espresso all'interno dello spazio di Hilbert.

Partiamo dal caso unitario: Abbiamo già visto nel paragrafo 1.3 come un singolo qubit può trovarsi in una sovrapposizione degli stati fondamentali (anche detti *stati quantistici puri*, che avevamo indicato con $|0\rangle$ e $|1\rangle$), rappresentata come:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.1)$$

discutendone inoltre la probabilità.

Notiamo agevolmente come lo stato del intero sistema ($|\Psi\rangle$) è rappresentato da un prodotto tensoriale dei singoli stati puri dei qubit.

Il passaggio ai sistemi multi-qubit viene dunque automatico.

Consideriamo ad esempio come un sistema a due qubit possa trovarsi nello stato

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \quad (2.2)$$

dove $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, rappresentano i quattro possibili stati quantistici puri

dei due qubit.

Manipolando ed evolvendo lo stato quantistico, con porte e operazioni quantistiche, è possibile sfruttare il potere del principio di sovrapposizione e del entanglement per eseguire calcoli complessi come il Boson Sampling.

Ora che abbiamo una discreta familiarità con il concetto di stato quantistico, proseguiamo enunciandone le tipologie principalmente utilizzate nel campo del Boson Sampling, soffermandoci con attenzione su due di esse: la base di Fock, trattata nel sottoparagrafo seguente, e lo stato gaussiano, introdotto di seguito e dettagliatamente discusso in (2.2.1).

2.1.1.3 Base di Fock

Nella fotonica integrata, uno stato di Fock (o Base di Fock) è uno spazio di Hilbert (definito come lo spazio di Hilbert \mathbf{H}) che si riferisce a una configurazione in cui ogni canale di ingresso del circuito ottico contiene esattamente un fotone.

Uno stato di Fock $|\mathbf{n}\rangle$ rappresenta uno stato con esattamente n fotoni, dove n è un numero intero non negativo. Ad esempio lo stato $|\mathbf{0}\rangle$ corrisponde allo stato di vuoto, che rappresenta l'assenza di fotoni. Lo stato $|\mathbf{1}\rangle$ rappresenta uno stato a singolo fotone, $|\mathbf{2}\rangle$ rappresenta uno stato con due fotoni e così via.

Se ci sono tre canali di input, l'input dello stato di Fock potrebbe essere rappresentato come $|\mathbf{1}, \mathbf{1}, \mathbf{1}\rangle$, indicando un fotone in ciascun canale.

Altri stati di input sono: -lo stato di ingresso a fotone singolo, in cui solo un canale di ingresso contiene un fotone, mentre gli altri sono nello stato di vuoto $|\mathbf{0}\rangle$ (nessun fotone). Ad esempio, in una configurazione a tre canali, uno stato di ingresso di un singolo fotone potrebbe essere rappresentato come $|\mathbf{1}, \mathbf{0}, \mathbf{0}\rangle$.

-lo stato di input randomizzato, che assume distribuzioni probabilistiche di fotoni attraverso i canali di input, consentendo ai ricercatori di studiare l'impatto della casualità sulla distribuzione di output.

-lo stato gaussiano, trattato ampiamente nel paragrafo 2.2.1.

2.1.2 Rete ottica

Diamo ora una descrizione generale della rete ottica che rende possibile il Boson Sampling.

- **Sorgente:** Il primo componente del circuito ottico è rappresentato da una sorgente di singoli fotoni. Questi possono essere generati utilizzando vari metodi come la *spontaneous parametric down conversion* (SPDC), proprietà

dei cristalli non lineari o da emettitori di fotoni singoli. L'obiettivo è avere una sorgente ben controllata che produca fotoni indistinguibili.

- **Implementatori di stato:** Nel paragrafo precedente si è ampiamente discusso dell'importanza della preparazione dello stato di input, che può essere implementato utilizzando fibre ottiche, guide d'onda o altre strutture.
- **Divisori di fascio:** Elementi fondamentali del circuito ottico sono i divisori di fascio (*Beam splitters*), che hanno il compito di separare e ricombinare i percorsi dei fotoni, consentendo effetti di interferenza. Quando la luce colpisce la superficie parzialmente riflettente di un divisore di fascio, una parte della luce viene trasmessa attraverso la superficie e un'altra parte viene riflessa. L'esatto rapporto di divisione dipende dalle caratteristiche del divisore di raggio, come il rivestimento utilizzato sulla superficie, i più comuni implementano un rapporto di 50:50.
- **Sfasatori:** Altri elementi indispensabili sono gli sfasatori, che vengono utilizzati per introdurre cambiamenti di fase controllati nei percorsi ottici. Possono essere implementati utilizzando varie tecniche, come la regolazione della lunghezza del percorso o l'utilizzo di modulatori elettro-ottici. Gli sfasatori consentono il controllo delle differenze di fase relative tra diversi percorsi di fotoni, aspetto cruciale per gli effetti di interferenza.
- **Rilevatori:** All'uscita del circuito, vengono posizionati dei rivelatori, utilizzati per misurare la presenza o l'assenza di fotoni e possono essere implementati utilizzando rivelatori a fotone singolo, come fotodiodi a valanga o rivelatori di nanofili superconduttori. I rivelatori forniscono informazioni sulla distribuzione dei fotoni e vengono utilizzati per dedurre l'esito dell'esperimento di campionamento dei bosoni.

È importante notare che il circuito ottico utilizzato nel Boson Sampling è distinto dai circuiti ottici universali utilizzati nel calcolo quantistico generico, in quanto il Boson Sampling si basa sull'interferenza di bosoni identici e non mira a risolvere problemi computazionali generali, ma piuttosto a dimostrare un vantaggio quantistico in scenari specifici.

2.1.3 Interferenza e misurazione

La luce, inclusi i fotoni, mostra proprietà sia di particelle che di onde (*dualità onda-particella*). In quanto particelle, i fotoni sono entità discrete che trasportano energia e quantità di moto, tuttavia, presentano anche caratteristiche ondulatorie, come l'interferenza e la diffrazione, che sono fondamentali per l'interferenza quantistica. Fenomeni di interferenza quantistica sono stati dimostrati attraverso l'esperimento della doppia fenditura, a tal proposito è bene ricordare che vale ancora il principio di sovrapposizione, ampiamente discusso assieme all'esperimento della doppia fenditura nel paragrafo 1.1. Nel Boson Sampling i fotoni sono soggetti a tale fenomeno, infatti, a causa della loro natura indistinguibile, possono interferire l'uno con l'altro, determinando schemi di interferenza complessi alle porte di uscita. Tali modelli di interferenza, sono caratterizzati da regioni di maggiore o minore probabilità di rilevamento dei fotoni, in quanto quando si incontrano o interferiscono tra loro, le loro ampiezze di probabilità interferiscono l'una con l'altra.

Questi modelli dipendono dalla configurazione specifica della rete e dallo stato di input iniziale dei fotoni, in ogni caso possiamo descrivere solo due fenomeni di interferenza quantistica:

- **Interferenza costruttiva:** L'interferenza costruttiva si verifica quando le ampiezze di probabilità dei fotoni si allineano e si rafforzano a vicenda. In questo caso, le ampiezze si sommano, determinando una maggiore probabilità di rilevare fotoni in determinate regioni, producendo frange luminose o regioni di alta intensità nel modello di interferenza.
- **Interferenza distruttiva:** l'interferenza distruttiva si verifica quando le ampiezze di probabilità dei fotoni si oppongono l'una all'altra. Le ampiezze si annullano, portando a una minore probabilità di rilevare fotoni in determinate regioni, producendo frange oscure o regioni di bassa intensità nel modello di interferenza.

Misurando dunque la distribuzione dei fotoni alle porte di uscita, è possibile estrarre informazioni sui modelli di interferenza e sulle probabilità di uscita associate a diverse configurazioni di fotoni. La sfida computazionale sta nel calcolare in modo efficiente queste probabilità di output, che crescono in modo esponenziale con il numero di fotoni e la dimensione della rete.

2.1.4 Distribuzione di probabilità

La distribuzione di probabilità dei risultati è determinata dai modelli di interferenza e dipende dalla disposizione specifica del circuito ottico e dallo stato di ingresso. Le interazioni bosoniche lineari, o reti di scattering lineare, sono definite dalle dinamiche

nell'immagine di Heisenberg che generano una relazione lineare tra gli operatori di annichilimento di ciascuna modalità. Cioè, solo quegli operatori unitari \mathcal{U} che agiscono sulla base di Fock in modo tale che

$$\mathcal{U}^\dagger \mathbf{a}_i \mathcal{U} = \sum_j \mathbf{u}_{ij} \mathbf{a}_j \quad (2.3)$$

dove \mathbf{a}_i è l'operatore di annichilimento dell' i -esimo modo e \mathbf{u}_{ij} forma una *scattering matrix* o *Unitary matrix* che per m modi è una matrice $\mathbf{m} \times \mathbf{m}$. È importante fare una distinzione tra l'operatore unitario \mathcal{U} che agisce sulla base di Fock e la *Unitary matrix* definita da \mathbf{u}_{ij} che descrive l'interferenza lineare dei modi. Per i sistemi ottici la matrice \mathbf{u}_{ij} è determinata esclusivamente da come sono disposti gli elementi ottici lineari, come i divisori di fascio e gli sfasatori.

2.1.4.1 Scattering matrix o Unitary matrix

Tali modelli di interferenza possono essere espressi attraverso una matrice, che prende il nome di *Scattering matrix* o *Unitary matrix*. In particolare essa rappresenta le ampiezze di probabilità dei fotoni di traslare da una determinata modalità di input ad un'altra modalità di output.

Cerchiamo di introdurre un esempio estremamente semplificato ed esclusivamente illustrativo supponendo di condurre un esperimento di Boson Sampling con 3 stati di input e 3 stati di output di conseguenza la matrice di scattering \mathbf{U} , avrà dimensione $\mathbf{3} \times \mathbf{3}$. Ogni elemento \mathbf{u}_{ij} della matrice rappresenta l'ampiezza di probabilità di un fotone che passa dallo stato di input \mathbf{i} allo stato di output \mathbf{j} . Un esempio di tale matrice potrebbe essere il seguente:

$$\mathbf{U} = \begin{bmatrix} 0.7 & 0.3 & 0 \\ 0.4 & 0.5 & 0.6 \\ 0 & 0.8 & 0.6 \end{bmatrix} \quad (2.4)$$

È evidente come la definizione di tale matrice renda implicito che la somma degli elementi di ogni riga debba essere 1. Tale matrice gioca un ruolo cruciale nel Boson Sampling, in quanto a partire da essa è possibile calcolare la distribuzione di probabilità di specifiche sequenze di fotoni in uscita dal circuito.

Di seguito è fornita una rappresentazione schematica di un'istanza a $\mathbf{n}=5$ fotoni e $\mathbf{m}=32$ modalità del problema di Boson Sampling, in modo da evidenziare il ruolo della *scattering matrix*. Partendo da sinistra vediamo come i 5 fotoni (rappresentati da pallini rossi) vengano iniettati individualmente nelle modalità di input, interagiscano linearmente attraverso una rete lineare associata ad una *scattering matrix* \mathbf{U} ,

controllata in modo classico (rappresentata in basso) ed infine tutte le uscite (a destra) vengono rilevate nella base di Fock.

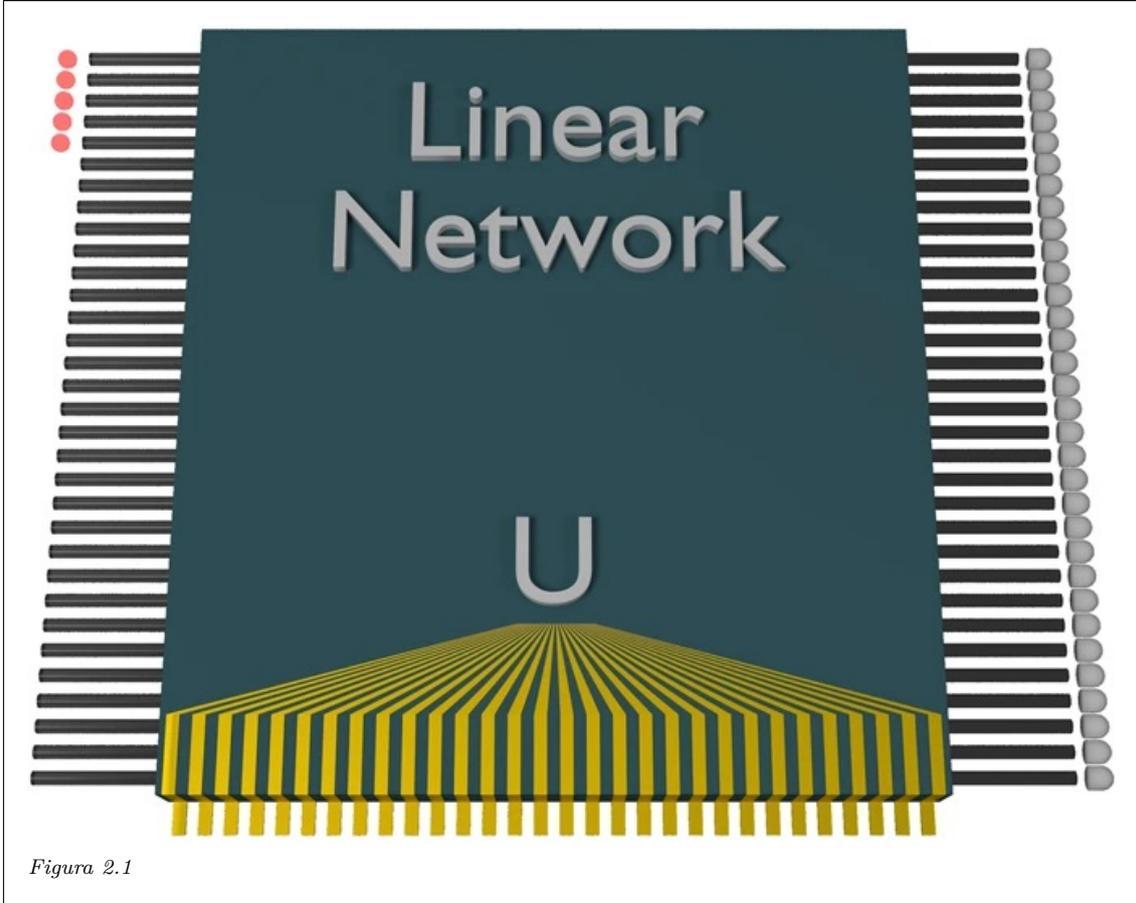


Figura 2.1: Rappresentazione schematica di un'istanza a 5 fotoni e 32 modalità del problema di Boson Sampling

La distribuzione di probabilità degli eventi in uscita è correlata al Permanente di sottomatrici di \mathbf{u}_{ij} . La matrice Permanente è definita in modo ricorsivo come il comune Determinante di matrice, ma senza l'alternanza di addizione e sottrazione.

2.1.4.2 Permanente della scattering matrix

Prima di analizzare come esso giochi un ruolo cruciale nel calcolo delle distribuzioni di probabilità, è bene definire matematicamente il Permanente di una matrice, e per farlo ci avvalremo della *formula di Leibniz*.

Definizione 2 (Permanente). Data una matrice quadrata $\mathbf{A} = [\mathbf{a}_{ij}]$ di dimensione $\mathbf{n} \times \mathbf{n}$, il Permanente, indicato con $\mathbf{perm}(\mathbf{A})$, è definito come:

$$\mathbf{perm}(\mathbf{A}) = \sum_{\sigma \in S_n} \prod_{i=1}^n \mathbf{a}_{i,\sigma(i)} \quad (2.5)$$

dove σ_i rappresenta una permutazione, ovvero un elemento del gruppo simmetrico \mathbf{S}_n , e σ_i indica l'i-esimo elemento della permutazione.

Analizzando la definizione (2), è immediato notare la somiglianza con quella di Determinante di una matrice:

Definizione 3 (Determinante). Data una matrice quadrata $\mathbf{A} = [\mathbf{a}_{ij}]$ di dimensione $\mathbf{n} \times \mathbf{n}$, il Determinante, indicato con $\mathbf{det}(\mathbf{A})$, è definito come:

$$\mathbf{perm}(\mathbf{A}) = \sum_{\sigma \in \mathbf{S}_n} \mathbf{sgn}(\sigma) \prod_{i=1}^n \mathbf{a}_{i,\sigma(i)} \quad (2.6)$$

dove ancora una volta \mathbf{S}_n è l'insieme simmetrico di tutte le permutazioni, mentre $\mathbf{sgn}(\sigma)$ denota il segno della permutazione ($+1$ se σ è una permutazione pari, -1 se è dispari), $\sigma(i)$ indica l'i-esimo elemento della permutazione.

La differenza sostanziale tra Permanente e Determinante di una matrice, sta dunque nel segno della permutazione, infatti, mentre il primo somma tutti i termini con segno positivo, nel secondo il segno dei termini dipende della posizione della permutazione.

Esempio 1. Data una matrice quadrata $\mathbf{A} = [\mathbf{a}_{ij}]$ di dimensione $\mathbf{3} \times \mathbf{3}$, definita come segue:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad (2.7)$$

Il Permanente di tale matrice è definito come:

$$\begin{aligned} \mathbf{perm}(\mathbf{A}) = & \mathbf{a}_{1,\sigma(1)}\mathbf{a}_{2,\sigma(2)}\mathbf{a}_{3,\sigma(3)} + \mathbf{a}_{1,\sigma(1)}\mathbf{a}_{2,\sigma(3)}\mathbf{a}_{3,\sigma(2)} \\ & + \mathbf{a}_{1,\sigma(2)}\mathbf{a}_{2,\sigma(1)}\mathbf{a}_{3,\sigma(3)} + \mathbf{a}_{1,\sigma(2)}\mathbf{a}_{2,\sigma(3)}\mathbf{a}_{3,\sigma(1)} \\ & + \mathbf{a}_{1,\sigma(3)}\mathbf{a}_{2,\sigma(1)}\mathbf{a}_{3,\sigma(2)} + \mathbf{a}_{1,\sigma(3)}\mathbf{a}_{2,\sigma(2)}\mathbf{a}_{3,\sigma(1)} \end{aligned} \quad (2.8)$$

Al contrario del calcolo del Determinante che include contributi sia positivi che negativi e annulla molti termini, risultando un calcolo potenzialmente efficiente dal punto di vista computazionale, il Permanente è noto per essere un problema computazionalmente difficile per i computer classici, classificandolo come problema di difficoltà $\#P\text{-Hard}$, il che significa che è computazionalmente difficile e non risolvibile in modo efficiente per grandi matrici.[21][22]

Le classi di complessità forniscono un quadro per comprendere la difficoltà computazionale dei problemi e l'efficienza degli algoritmi che li risolvono, riferendosi a categorie che classificano i problemi computazionali in base alle risorse necessarie per risolverli. Esistono varie classi di complessità, denominate attraverso l'operatore $\#$.

E' bene inoltre precisare che l'interpretazione specifica di un valore alto o basso del Permanente dipende dal contesto e dallo specifico esperimento condotto. In generale, un valore elevato del Permanente indica un forte schema di interferenza e implica una maggiore probabilità di osservare effetti di interferenza complessi in output. Al contrario, un valore basso del Permanente (come in questo caso), indica un modello di interferenza più debole, suggerendo che i fotoni hanno meno probabilità di esibire effetti di interferenza complessi.

Supponiamo ora di disporre di uno stato di ingresso così definito:

$$\underbrace{|\mathbf{1}, \mathbf{1}, \mathbf{1}, \dots, \mathbf{1}\rangle}_n \underbrace{|\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}\rangle}_{m-n} \quad (2.9)$$

esso rappresenta uno *stato di Fock* \mathbf{m} modale a \mathbf{n} fotoni.

Lo stato si evolve attraverso la rete lineare e l'output è costituito da campioni dalla distribuzione risultante dalla misurazione sulla base Fock di tutte le modalità (di cui è stato espresso un esempio in *Fig. 2.1*). L'insieme degli eventi che vengono quindi emessi dall'algorithm è una sequenza di \mathbf{m} interi non negativi la cui somma è \mathbf{n} , denotata con $\phi_{\mathbf{m},\mathbf{n}}$.

Possiamo ora definire la distribuzione di probabilità in uscita dalla rete lineare relativa allo stato di ingresso appena definito. Per un evento $\mathbf{S} = (\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_n) \in \phi_{\mathbf{m},\mathbf{n}}$ in uscita dalla rete, la probabilità di \mathbf{S} è allora:

$$p_{\mathbf{S}} = \frac{|\mathbf{Per}(\mathbf{A}_{\mathbf{S}})|^2}{\mathbf{s}_1! \mathbf{s}_2! \dots \mathbf{s}_n!} \quad (2.10)$$

dove la matrice $\mathbf{A}_{\mathbf{S}}$ è una sottomatrice $\mathbf{n} \times \mathbf{n}$ di \mathbf{u}_{ij} dove la riga \mathbf{i} è ripetuta \mathbf{s}_i volte e sono utilizzate solo le prime \mathbf{n} colonne.

E' bene precisare come il fatto che ogni probabilità sia derivata dal Permanente di una sottomatrice della stessa *Unitary matrix* garantisce che tutte le probabilità siano inferiori a 1 e la distribuzione sia normalizzata.

Ci si accorge allora immediatamente di come la difficoltà del calcolo della probabilità relativa a tutti i possibili $\binom{\mathbf{m}}{\mathbf{n}}$ eventi di $\phi_{\mathbf{m},\mathbf{n}}$ in uscita dal sistema cresca molto rapidamente in maniera esponenziale. Una dimostrazione temporale sarà fornita le paragrafo 3.3.3.

Nell'ambito del Boson Sampling il calcolo del Permanente svolge un ruolo fondamentale poiché cattura i modelli di interferenza e rappresenta la complessità della simulazione delle distribuzioni di output osservate. La sua complessità computazionale, la connessione all'interferenza quantistica e l'analisi della complessità contribuiscono a evidenziare come sistemi quantistici in grado di trattare il problema del Boson

Sampling, siano capaci di raggiungere il vantaggio quantistico.

Un altro aspetto non accuratamente approfondito nella stesura, ma altrettanto cruciale nel Boson Sampling è di preservare la natura quantistica dei fotoni durante il calcolo, poiché qualsiasi interazione indesiderata o perdita di coerenza può influenzare il risultato finale. Rumore, imperfezioni nei componenti ottici e altre limitazioni sperimentali possono degradare la qualità dell'informazione trasportata dal fotone. È quindi importante notare che il Boson Sampling non è stato ancora dimostrato con un elevato numero di fotoni anche a causa appunto dei severi requisiti per sorgenti di fotoni precise, componenti ottici a bassa perdita e tecniche di rilevamento efficienti. E' doveroso sottolineare anche come il Boson Sampling non sia un modello universale di calcolo quantistico come le macchine di Turing quantistiche o i circuiti quantistici universali, ma rappresenti un problema specifico che rivela la potenziale forza computazionale dei sistemi quantistici esclusivamente in determinati scenari. Infine esso ad oggi non trova vere e proprie applicazioni pratiche al di fuori del suo utilizzo per testare compilatori quantistici o per la dimostrazione del *quantum supremacy*.

2.2 Gaussian Boson Sampling (GBS)

Il Gaussian Boson Sampling (GBS) rappresenta un'estensione al problema originale del Boson Sampling (2.1), consentendo agli stati di input (2.1.1.2) di essere stati gaussiani (2.2.1) arbitrari anziché essere limitati agli stati di Fock (2.1.1.3).

[23] Il vantaggio nell'utilizzo degli stati gaussiani è che la distribuzione di probabilità degli stati di uscita in GBS può essere calcolata in modo efficiente utilizzando l'Hafniano di una matrice, che è computazionalmente più semplice del Permanente. Inoltre, i pattern di interferenza generati dagli stati gaussiani sono più semplici rispetto a quelli del classico Boson Sampling. Questa semplificazione consente simulazioni e calcoli più efficienti.

E' importante sottolineare però che le semplificazioni apportate in GBS non impediscono l'utilizzo di tale procedura per il raggiungimento del vantaggio quantico, in quanto è stato ampiamente dimostrato che il calcolo dell'Hafniano è un'operazione appartenente al livello di complessità $\#P\text{-Hard}$ [23], già trattato nel paragrafo precedente.

2.2.1 Stati Gaussiani

Gli stati gaussiani prendono il nome dalla funzione di distribuzione di probabilità che li descrive, essendo quest'ultima di forma appunto gaussiana. Essi inoltre rappresentano una classe di stati quantistici le cui proprietà sono completamente caratterizzate dalla loro descrizione del primo e del secondo ordine (Vettore della media, e matrice di

covarianza). Tale caratterizzazione degli stati gaussiani fornisce un modo conciso ed efficiente dal punto di vista computazionale per determinarne completamente lo stato.

Gli stati gaussiani sono ampiamente utilizzati non solo per la loro descrizione relativamente semplice, ma anche per le loro proprietà particolarmente vantaggiose:

- **Stabilità sotto trasformazioni lineari:** gli stati gaussiani rimangono gaussiani quando sottoposti a trasformazioni lineari come operazioni unitarie, attraversamento di divisori di fascio e sfasatori. Questa proprietà semplifica la loro analisi e manipolazione.
- **Incerteza minima:** alcuni stati gaussiani, denominati *stati gaussiani coerenti* saturano il principio di indeterminazione, nel senso che raggiungono la minima incerteza possibile nella posizione e nella quantità di moto osservabili.
- **Facile "preparazione" e rilevamento:** gli stati gaussiani possono essere facilmente "preparati" (ad esempio in uno stato di sovrapposizione) e misurati in molti sistemi fisici, compresi i campi ottici. Tecniche di manipolazione di stati quantistici della luce, come le operazioni di squeezing, beam splitting e displacement possono generare e manipolare stati gaussiani.

Nello specifico, il metodo di squeezing per la generazione e la manipolazione degli stati gaussiani sarà di interesse per il proseguimento della trattazione del capitolo e per la trattazione del capitolo successivo.

2.2.2 Squeezed light

Nella ottica quantistica, il termine squeezed light si riferisce a un tipo specifico di luce che presenta un rumore quantico ridotto in una delle quadrature del campo elettromagnetico in cui avviene la compressione. In questo modo è possibile migliorare la sensibilità degli interferometri, migliorare il rapporto segnale-rumore nelle misurazioni quantistiche e consentire una manipolazione più precisa delle informazioni.

Con rumore quantico ci si riferisce alle fluttuazioni e alle incertezze intrinseche che sorgono a causa della natura quantistica dei sistemi in esame.

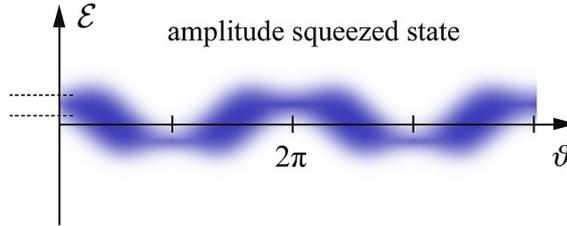
Il rumore quantico nasce dal principio di indeterminatezza, che afferma che l'osservazione a coppie di proprietà osservabili, come posizione e quantità di moto o energia e tempo, non possono essere conosciute simultaneamente con precisione arbitraria. Il principio di indeterminazione implica che anche in un sistema quantistico perfettamente controllato e isolato, ci saranno sempre inevitabili fluttuazioni e incertezze nelle quantità misurate.

L'operazione di compressione dunque ridistribuisce efficacemente il rumore quantico,

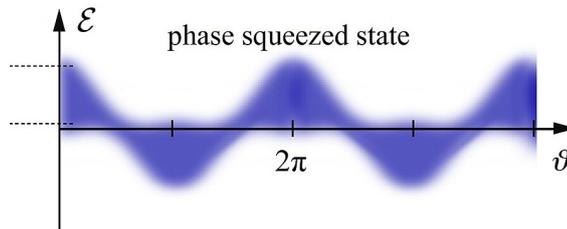
con conseguente riduzione del rumore in una quadratura del campo elettromagnetico a scapito però di un aumento del rumore nella quadratura coniugata.

Possiamo allora ridurci a due modalità di luce compressa:

- **Amplitude squeezing:** in questa modalità, l'ampiezza del campo elettrico della luce compressa viene ridotta al di sotto del limite quantistico standard (SQL). Significa che il rumore nell'ampiezza della luce è ridotto al di sotto di quanto ci si aspetterebbe classicamente.



- **Phase Squeezing:** in questa modalità, è la fase del campo elettrico della luce ad essere compressa al di sotto dell'SQL. In questo modo il rumore nella fase della luce viene ridotto, consentendo misurazioni e manipolazioni di fase più precise.



Possiamo allora realizzare uno stato gaussiano, partendo da uno stato di vuoto $|\mathbf{0}\rangle$, rappresentante l'assenza di fotoni e applicando un'operazione di squeezing in una delle quadrature del campo elettromagnetico, tipicamente implementato utilizzando un *amplificatore parametrico* o un *crystallo non lineare*. L'operatore di compressione, indicato come $\mathcal{S}(\mathbf{r}, \phi)$, può essere scritto come:

$$\mathcal{S}(\mathbf{r}, \phi) = e^{(\mathbf{r}/2)(\alpha^{\dagger 2}e^{-i\phi} - \alpha e^{i\phi})} \quad (2.11)$$

dove α^{\dagger} e α sono gli operatori di creazione e annichilimento, \mathbf{r} è il parametro che determina la quantità di compressione e ϕ è l'angolo che determina la direzione di compressione nello spazio di quadratura.

Applicando tale operazione allo stato di vuoto si ottiene lo stato compresso:

$$|\Psi\rangle = \mathcal{S}(\mathbf{r}, \phi)|\mathbf{0}\rangle \quad (2.12)$$

$|\Psi\rangle$ sarà uno stato gaussiano con incertezza ridotta nella quadratura compressa e

maggiore incertezza nella quadratura coniugata.

Una volta introdotti questi concetti lo svolgimento del problema di GBA è analoga a quella del generico Boson Sampling, descritto in 2.1, dove i fotoni attraversano una rete ottica 2.1.2, in cui si verifica il fenomeno dell'interferenza quantistica 2.1.3, per poi rilevare in uscita una serie di sequenze di fotoni ben distinte, ognuna delle quali descritta da una distribuzione di probabilità.

La vera novità introdotta da GBS è che la probabilità di misurare una specifica distribuzione di output di fotoni da uno stato gaussiano generale può essere espressa utilizzando una funzione di matrice chiamata Hafniano, decisamente meno complicato da calcolare rispetto al Permanente 2.

2.2.3 Hafniano della Scattering matrix

Equivalentemente all'analogia tra Permanente e Determinante, anche l'Hafniano, in cui i segni delle permutazioni non vengono prese in considerazione, presenta una controparte, che prende il nome di Pfaffiano, dove vengono appunto considerati i segni delle permutazioni.

Definizione 4 (Hafniano). Data una matrice quadrata $\mathbf{A} = [\mathbf{a}_{ij}]$ di dimensione $\mathbf{n} \times \mathbf{n}$, l'Hafniano, indicato con $\mathbf{haf}(\mathbf{A})$, è definito come:

$$\mathbf{haf}(\mathbf{A}) = \frac{1}{\mathbf{n}!} \sum_{\sigma \in \mathbf{S}_n} \prod_{i=1}^n a_{\sigma(i-1), \sigma(i)} \quad (2.13)$$

dove σ_i rappresenta una permutazione, ovvero un elemento del gruppo simmetrico \mathbf{S}_n , e σ_i indica l' i -esimo elemento della permutazione.

La discussione del ruolo del'haffiano in GBS, richiederebbe una lunga complessa trattazione, che però non farò, ma che è consultabile in [23]. Mi limiterò invece a sottolineare come Il calcolo Hafniano fornisca le ampiezze di probabilità associate a diverse configurazioni di output dei fotoni, analogamente a quanto visto nel Boson Sampling. Introduciamo ora un importante risultato secondo cui è possibile ricavare il Permanente di una matrice, attraverso il calcolo del'Hafniano, in particolare vale:

$$\mathbf{per}(\mathbf{A}) = \mathbf{haf} \begin{pmatrix} & \mathbf{A} \\ \mathbf{A}^T & \end{pmatrix} \quad (2.14)$$

Ciò consente di dimostrare, che anche il calcolo del'Hafniano di una matrice è un'operazione appartenente al livello di complessità $\#P\text{-Hard}$, di cui fa parte anche il calcolo del Permanente. In questo modo Anche GBS può essere considerato un metodo valido per dimostrare il vantaggio quantistico di un sistema computazionale.[23]

2.3 Obiettivi di GBS

Dall'analisi fatta su GBS e più in generale il Boson Sampling, giungiamo a concludere che entrambi puntano a dimostrare la superiorità del calcolo quantistico rispetto al calcolo classico arrivando a mettere in discussione persino il teorema di Church-Turing, il tutto per di più senza richiedere la definizione di un computer quantistico universale.

2.3.1 Teorema esteso di Church-Turing

Il teorema di Church-Turing esteso, noto anche come principio di Church-Turing-Deutsch, è un concetto di importante rilevanza nell'informatica teorica e nel calcolo quantistico, esso ha un ruolo cruciale nel plasmare il campo dell'informatica quantistica, fornendo una base teorica e stabilendo i confini di ciò che è computazionalmente realizzabile. Sottolinea l'importanza del calcolo classico come quadro universale e pone le basi per confrontare le capacità computazionali di diversi modelli di calcolo. Esso afferma che qualsiasi dispositivo di calcolo realizzabile fisicamente, operante all'interno delle leggi della fisica come le intendiamo attualmente, può essere simulato in modo efficiente da una macchina di Turing. In altre parole, la Tesi di Church-Turing suggerisce che l'insieme dei problemi risolvibili da una macchina di Turing rappresenti i limiti della computabilità. Ciò significa che sebbene possano esserci diverse implementazioni fisiche del calcolo (ad esempio, computer classici, computer quantistici, computer analogici), alla fine sono tutti equivalenti in termini di potenza di calcolo. Il teorema inoltre afferma che i computer quantistici, nonostante il loro potenziale per risolvere determinati problemi in modo più efficiente rispetto ai computer classici, non possono risolvere problemi che sono fondamentalmente non calcolabili con mezzi classici. Pertanto, sebbene i computer quantistici offrano vantaggi significativi per determinati compiti, non violano la tesi di Church-Turing.

Tuttavia è importante notare che GBA e più in generale il Boson Sampling non dimostrano la superiorità quantistica rispetto al calcolo classico in generale, in quanto entrambi rappresentano problemi sì computazionalmente difficili, ma estremamente specifici, non comprendendo l'intera gamma di problemi computazionali che i computer quantistici sono in grado di risolvere in modo efficiente.

Ed ecco che Borealis, che verrà ampiamente trattato nel prossimo capitolo, rappresenta un punto di svolta nella dimostrazione della superiorità quantistica rispetto al calcolo classico, in quanto esso è un processore fotonico che offre programmabilità dinamica su tutte le porte implementate, effettuando il GBS su 216 modalità di input.

Capitolo 3

Il processore quantico fotonico Borealis

Borealis è un processore quantico fotonico realizzato dall'azienda canadese Xanadù che offre programmabilità dinamica su tutte le porte implementate, effettuando GBS con un massimo di 219 fotoni su un input di 216 stati di luce compressa (*squeezed light* (2.2.2)) correlati in una disposizione spaziale tridimensionale, attraverso un'architettura di *time domain multiplexing* (TDM (3.1.1)) e rilevamento del numero di fotoni con elevata precisione attraverso un'architettura *photon number resolving*.

Tale configurazione offre potenze di calcolo mai raggiunte prima, in particolare è stato dimostrato come in media occorrerebbero più di 9000 anni ai migliori algoritmi e supercomputer disponibili per produrre, utilizzando metodi esatti, un singolo campione dalla distribuzione di probabilità in uscita dal sistema, mentre, Borealis richiede solo 36 μs , risultato ben 50 milioni di volte migliore di quello riportato dalle precedenti macchine fotoniche. [24]

Ci si pone dunque come ambizioso obiettivo il raggiungimento del vantaggio computazionale quantistico superando così qualsiasi computer classico che esegua algoritmi noti su compiti ben definiti.

Fino ad ora infatti nessuna macchina fotonica che offra programmabilità su tutte le porte aveva dimostrato un vantaggio computazionale quantistico, in quanto esperimenti precedentemente condotti attraverso altri sistemi fotonici erano in gran parte limitati a sequenze di porte statiche e vulnerabili allo spoofing, tecnica atta alla manipolazione delle informazioni.

Questo lavoro è una pietra miliare fondamentale nel percorso verso un computer quantistico pratico, convalidando le caratteristiche tecnologiche chiave della fotonica come piattaforma per questo obiettivo.

3.1 Overview del Progetto

Solo una manciata di esperimenti ha utilizzato dispositivi quantistici per svolgere compiti computazionali che siano al di fuori della portata dei computer classici odierni. In tutti questi, il compito computazionale ha comportato il campionamento da distribuzioni di probabilità che, come già visto nel capitolo precedente, è ritenuto essere esponenzialmente difficile da simulare utilizzando il calcolo classico.

Una di queste dimostrazioni si basava su un processore superconduttore programmabile a 53 qubit, mentre un'altra utilizzava una piattaforma fotonica non programmabile che implementava il GBS con 50 stati compressi inseriti in un interferometro statico casuale a 100 modalità. Entrambi sono stati seguiti a breve da versioni migliori, rispettivamente con più qubit e un maggiore controllo sulla luminosità e un set limitato di parametri del circuito.

Questi esperimenti hanno posto le rispettive piattaforme all'interno del regime del vantaggio computazionale quantistico, sebbene ne manchi ancora una dimostrazione che garantisca anche la solidità della piattaforma agli errori. [24]

3.1.1 Time Domain Multiplexing (TDM)

TDM è un approccio utilizzato nella realizzazione di sistemi quantistici atto solitamente ad aumentare il numero di qubit. In uno schema di multiplexing nel dominio del tempo, una singola risorsa hardware fisica, come una linea di controllo o un impulso di controllo, è condivisa nel tempo tra più qubit. Ogni qubit viene indirizzato e manipolato durante la sua finestra temporale designata. Coordinando attentamente i tempi delle operazioni, i qubit possono essere controllati individualmente anche se condividono la stessa risorsa fisica. Questa tecnica è particolarmente rilevante nei sistemi in cui le singole linee di controllo o gli impulsi di controllo per ogni qubit sarebbero impraticabili a causa delle limitazioni delle risorse hardware o della complessità di fabbricazione. Il multiplexing nel dominio del tempo fornisce un modo per superare queste limitazioni utilizzando in modo efficiente una risorsa di controllo condivisa. [25]

Nella fotonica integrata, il multiplexing nel dominio del tempo (TDM) offre quindi un percorso relativamente efficiente in termini di hardware per costruire computer quantistici tolleranti ai guasti, codificando infatti le informazioni in impulsi di luce sequenziali e multiplexando efficacemente un piccolo numero di canali ottici per elaborare le informazioni su un gran numero di modalità; è possibile così disporre di stati grandi e altamente correlati con un numero relativamente piccolo di componenti ottici.

Ciò disaccoppia il numero di componenti richiesto e l'estensione fisica della macchina dalla dimensione del circuito quantistico in esecuzione; a condizione che le imperfezioni del dispositivo possano essere mantenute sufficientemente piccole, questo disaccoppiamento rappresenta un vantaggio sostanziale per la scalabilità. A tal proposito sebbene sia attraente per la scalabilità, l'efficienza del hardware non deve però introdurre errori inaccettabilmente grandi, quindi le implementazioni di TDM devono essere testate in contesti impegnativi per convalidare la loro premessa di realizzazione di computer quantistici praticamente efficienti.

Garantito ciò, i vantaggi forniti dal TDM come il numero relativamente modesto di percorsi ottici e componenti di controllo, consente di evitare molte delle sfide delle tradizionali implementazioni planari bidimensionali degli interferometri ottici, che soffrono di elevata complessità e gravosi requisiti di controllo parallelo. [24]

Utilizzando il multiplexing nel dominio del tempo, è stato possibile dunque generare deterministicamente grandi *cluster states* mono, bidimensionali e tridimensionali attraverso operazioni lineari programmabili, utilizzando un unico loop con fase riconfigurabile.[24]

3.1.2 Cluster States

I cluster state sono un'altra tipologia di stati (2.1.1.2), caratterizzati da una disposizione altamente correlata di qubit, che consente potenti capacità computazionali e facilita varie attività di informazione quantistica, come la correzione degli errori e il calcolo quantistico basato sulla misurazione.

Un cluster state è tipicamente rappresentato come un grafico o un reticolo di qubit, in cui ogni qubit è connesso ai suoi vicini tramite operazioni di entanglement. La struttura del grafico può variare a seconda della disposizione specifica e della connettività desiderate per una data applicazione, vediamo alcuni esempi utili alla comprensione del paragrafo.

- **Cluster States monodimensionali:** I cluster states monodimensionali, si riferiscono a un tipo specifico di stati in cui i qubit assumono una disposizione monodimensionale (retta), dove ogni qubit è correlato a quelli adiacenti nella stessa dimensione (sinistra, destra) tramite operazioni di entanglement.
- **Cluster States bidimensionali:** Nei cluster states bidimensionali, i qubit sono invece disposti in un reticolo bidimensionale o struttura a griglia in cui ogni qubit è correlato a quelli adiacenti (sinistra, destra, su e giù) tramite operazioni di entanglement.
- **Cluster States tridimensionali:** Sono la forma più avanzata di cluster states in cui i qubit sono disposti in una struttura a reticolo tridimensionale, di modo che ogni qubit sia correlato a quelli vicini al interno del reticolo, comprese anche le connessioni nella direzione verticale. La struttura di entanglement tridimensionale fornisce una connettività più ricca e consente calcoli quantistici più sofisticati.

Un'importante proprietà dei cluster states è che possiedono uno specifico schema di entanglement noto come entanglement dello stato del grafo che afferma che nel cluster state, l'entanglement non è localizzato tra i singoli qubit ma è distribuito nell'intero

sistema. Questa distribuzione dell'entanglement è ciò che consente la potenza e la versatilità dei cluster states per l'elaborazione delle informazioni quantistiche, misurando infatti in sequenza i qubit e utilizzando i risultati della misurazione come input per operazioni successive, è possibile eseguire calcoli esponenzialmente complessi. [26]

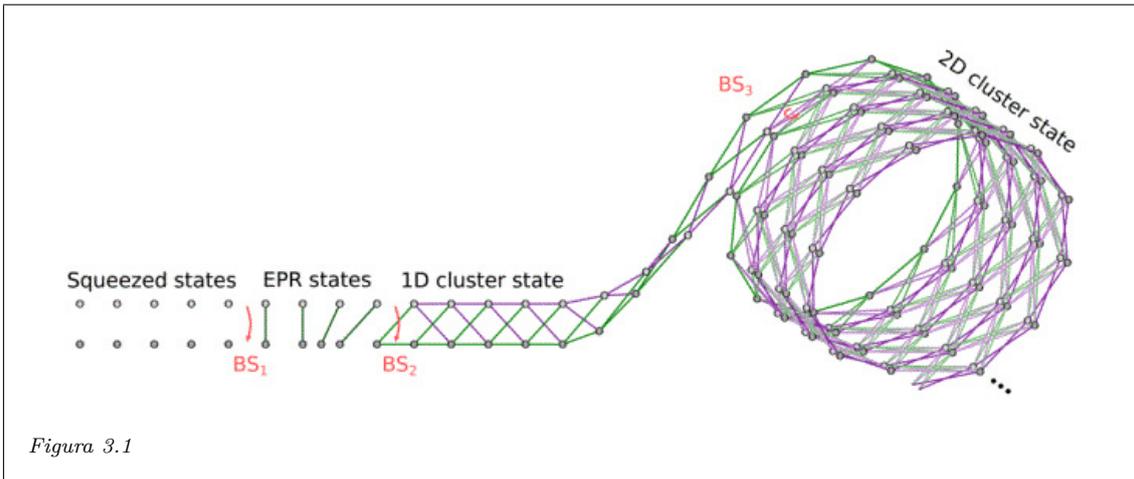


Figura 3.1: Rappresentazione dei cluster states.

Con questo lavoro, Xanadù risolve gli ostacoli tecnologici associati al TDM per l'implementazione di cluster states tridimensionali, alla commutazione elettro-ottica rapida, alla tecnologia di rilevamento del numero di fotoni ad alta velocità e alla generazione di luce compressa, per costruire un campionatore di bosoni gaussiano scalabile e programmabile, Borealis.

In questo modo, l'uso di TDM all'interno del campionatore consente di accedere a modalità più ridotte senza aumentare l'estensione fisica o la complessità del sistema, inoltre il dispositivo può essere facilmente programmato per la generazione di cluster states tridimensionali, selezionando appropriati rapporti di fase e di divisione del fascio nel circuito.

Grazie a queste implementazioni, Borealis utilizza 216 stati indipendenti per ottenere un vantaggio computazionale quantistico, ponendolo ben oltre le capacità degli attuali algoritmi di simulazione classica e sbloccando l'accesso a eventi di campionamento con un numero di fotoni totale molto grande, regime inaccessibile ai precedenti esperimenti.

3.2 Circuito ottico

L'ingresso dell'interferometro è formato da un singolo *oscillatore ottico parametrico* (OPO), che emette stati compressi monomodali a una frequenza di 6 MHz (clock) che vengono poi inviati a tre interferometri concatenati, programmabili e basati su loop.

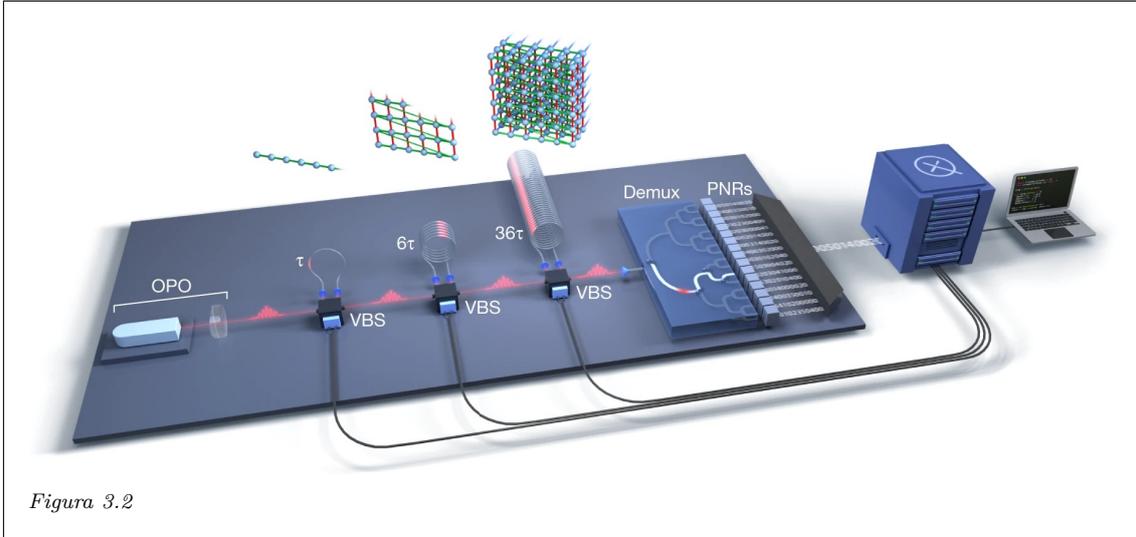


Figura 3.2

Figura 3.2: Circuito ottico che implementa Borealis.

Ogni loop contiene un VBS, incluso uno sfasatore programmabile, e una linea di ritardo in fibra ottica che funge da memoria buffer per la luce e consente l'interferenza di modi che sono temporalmente adiacenti $\tau = (6\text{MHz})^{-1}$ o avanti di 6 o 36 periodi temporali (6τ o 36τ) rispettivamente nel primo, secondo e terzo loop. I ritardi ottici forniscono un metodo compatto ed elegante per mediare accoppiamenti a corto e lungo raggio tra le modalità. Lo stato gaussiano multidimensionale generato per questo esperimento può essere visualizzato utilizzando una rappresentazione reticolare tridimensionale. Dato un reticolo di dimensione $\mathbf{a} = \mathbf{6}$, dove \mathbf{a} è il numero di modi che separano due impulsi correlati, nel secondo loop, si può formare un reticolo cubico iniettando $\mathbf{M} = \mathbf{a}^3 = \mathbf{216}$ impulsi di luce compressa nell'interferometro. Grazie al uso di una singola sorgente di luce compressa multiplexata nel tempo, tutte le modalità temporali sono, con ottima approssimazione, indistinguibili in tutti i gradi di libertà tranne ovviamente quella temporale e bloccate passivamente in fase l'una rispetto all'altra.

I campioni in uscita dai loop verranno poi parzialmente demultiplexati attraverso una rete di commutazione ad albero binario con 16 canali d'uscita, ciò consente di colmare il divario tra il clock a 6 MHz, scelto per mantenere lunghezze gestibili del loop in fibra, e il tempo di refresh dei rilevatori all'uscita del sistema. Tale rilevazione avviene utilizzando una serie di rilevatori di risoluzione del numero di fotoni (PNR) che garantiscono il **95%** di efficienza. [24]

3.3 Analisi dell'esperimento

Il circuito ottico appena descritto (*Fig. 3.1*) risulta essere completamente programmabile, fornendo un accoppiamento a lungo raggio tra diverse modalità e consentendo a tutti questi accoppiamenti di essere programmati dinamicamente. A differenza di alcuni algoritmi quantistici il cui corretto funzionamento su un computer quantistico può essere facilmente verificato utilizzando un computer classico, ciò non è possibile quando si ha a che fare con GBS.

L'esperimento consiste dunque nel provare che Borealis funzioni correttamente, cioè: campioni dalla distribuzione GBS specificata dalla matrice di trasferimento del dispositivo \mathbf{T} (equivalente alla scattering matrix (2.1.4.1)) e dal vettore dei parametri di compressione \mathbf{r} (già introdotto in (2.2.2)), che insieme definiscono il Ground Truth dell'esperimento.

Il termine *Ground Truth* spesso implica esperimenti e misurazioni attentamente controllati, in cui le proprietà note del sistema o i risultati attesi forniscono un riferimento per confrontare i risultati sperimentali.

In esperimenti precedenti i risultati venivano confrontati con un Ground Truth ottenuto da misurazioni tomografiche di un interferometro statico, mentre per Borealis il Ground Truth è rappresentato dai parametri \mathbf{T} e \mathbf{r} , specificati dall'utente.

Il parametro di compressione \mathbf{r} è definito dall'utente in base alla tipologia di esperimento da condurre, mentre la matrice \mathbf{T} è ottenuta combinando i tre loop di VBS che agiscono sui diversi modi, insieme alle perdite comuni (a tutti i modi) dovute alla propagazione e all'efficienza di fuga finita della sorgente, nonché alla trasmittanza imperfetta attraverso i sistemi di demultiplexing e rilevamento.

Se si volesse allora mirare ad un interferometro universale e programmabile, con profondità pari al numero di modi, l'accumulo esponenziale di perdita impedirebbe di mostrare un vantaggio quantistico. Ci sono quindi due modi per aggirare questo ostacolo: si può rinunciare alla programmabilità e costruire un interferometro statico fisso a bassissima perdita, o rinunciare all'universalità pur mantenendo un alto grado di entanglement multimodale utilizzando gate a lungo raggio.

3.3.1 Esecuzione dell'esperimento di campionamento con un basso numero di fotoni e modalità

Consideriamo innanzitutto il regime di pochi modi e un basso numero di fotoni, in cui è possibile raccogliere abbastanza campioni per stimare le probabilità attese, calcolandole anche dalla matrice di trasmissione \mathbf{T} e dal parametro di compressione

\mathbf{r} programmati nel dispositivo. Di seguito sono riportate le probabilità dedotte dai campioni casuali raccolti nell'esperimento confrontati con le probabilità per diversi campioni \mathbf{S} ottenuti dalle simulazioni, sotto le ipotesi di Ground Truth. [24]

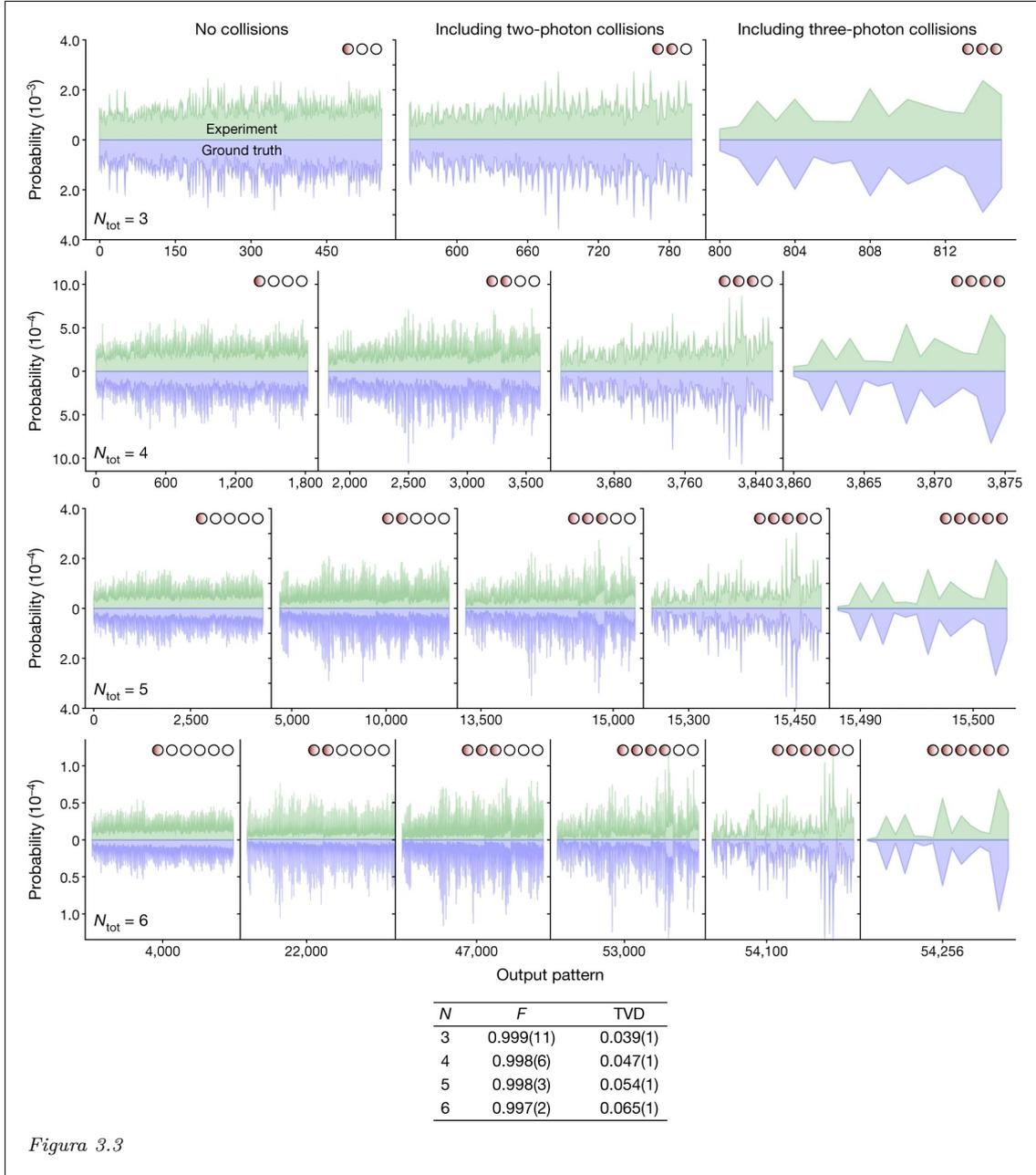


Figura 3.3: Dati relativi all'esperimento appena proposto, con numero di fotoni N crescente da 3 a 6.

Consideriamo tutte le possibili permutazioni in uscita, rappresentate da $\binom{N+M-1}{N}$ dove \mathbf{N} è il numero di fotoni, da 3 (numero minimo per osservare un fenomeno di interferenza) a 6, e $\mathbf{M}=16$ è il numero di modi. Per quantificare le prestazioni di Borealis calcoliamo la fedeltà (\mathbf{F}) e la distanza di variazione totale (\mathbf{TVD}) delle probabilità totali di numero di fotoni 3, 4, 5 e 6 relative al Ground Truth.

Per un numero totale di fotoni ben definito, (\mathbf{F}) e (\mathbf{TDV}) sono, rispettivamente, definiti come:

$$\mathbf{F} = \sum_i \sqrt{p_i q_i} \quad (3.1)$$

noto anche come coefficiente Bhattacharyya e

$$\mathbf{TV D} = \sum_i \frac{|p_i - q_i|}{2} \quad (3.2)$$

I parametri (\mathbf{p}_i) e (\mathbf{q}_i) rappresentano rispettivamente la probabilità teorica e sperimentale dell' i -esimo modello di output e sono normalizzati dalla probabilità del rispettivo numero totale di fotoni.

Per tutte le combinazioni totali di fotoni considerati si ottiene $\mathbf{F} \geq 99\%$ e $\mathbf{TDV} \leq 6,5\%$, dimostrando così che Borealis è ragionevolmente vicino al Ground Truth per un numero di fotoni \mathbf{N} basso.

E' doveroso considerare come, poiché il calcolo è effettuato su tutte le possibili probabilità con \mathbf{N} fotoni, la stima delle probabilità di esito dalla matrice \mathbf{T} caratterizzata sperimentalmente richiederebbe calcoli ben oltre le attuali capacità di elaborazione classica. Questa limitazione porta all'inevitabile crescita di $\mathbf{TV D}$ all'aumentare di \mathbf{N} e, oltre al costo computazionale poco pratico, è la ragione per cui si ferma ad $\mathbf{N}=6$.

3.3.2 Esecuzione dell'esperimento di campionamento con un numero moderato di fotoni e modalità

Vediamo ora come si comporta il sistema in un regime intermedio di numero di fotoni e modi.

Si procede calcolando l'entropia incrociata dei campioni generati dall'esperimento per ogni insieme totale di fotoni con $\mathbf{M}=216$ modi computazionali e numero di fotoni medio $\bar{\mathbf{N}}=21,120 \pm 0,006$.

Per un insieme di \mathbf{K} campioni $\{\mathbf{S}_i\}_{i=1}^{\mathbf{K}}$, ciascuno con un totale di \mathbf{N} fotoni, il calcolo dell'entropia sotto la verità fondamentale data da (\mathbf{r}, \mathbf{T}) fornisce:

$$\mathbf{X E}(\{\mathbf{S}_i\}_{i=1}^{\mathbf{K}}) = \sum_i^{\mathbf{K}} \ln \left(\frac{\mathbf{Pr}^{(0)}(\mathbf{S}_i)}{\mathcal{N}} \right) \quad (3.3)$$

dove

$$\mathcal{N} = \frac{\mathbf{Pr}^{(0)}(\mathbf{N})}{\binom{\mathbf{N}+\mathbf{M}-1}{\mathbf{N}}} \quad (3.4)$$

è una costante di normalizzazione determinata da come \mathbf{N} fotoni possono essere collocati in \mathbf{M} modi e $\mathbf{Pr}^{(0)}(\mathbf{N})$ è la probabilità di ottenere un totale di \mathbf{N} fotoni

sotto l'assunzione della verità fondamentale.

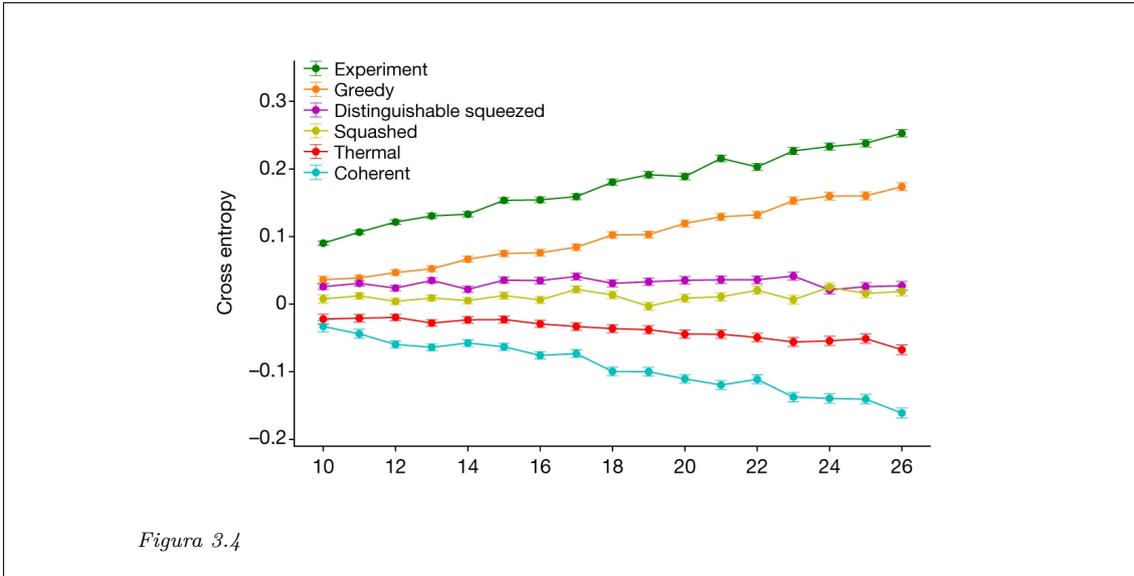


Figura 3.4

Figura 3.4: Confronto dei valori di entropia forniti dall'esperienza con quelli dei principali spoofer.

Si prosegue quindi confrontando il valore medio di entropia ottenuto con quello degli spoofer avversari che cercano di imitare la distribuzione di Ground Truth (r, T).

I cinque avversari considerati inviano: **Squeezed light**, **Thermal light**, **Coherent light**, **distinguishable light** nell'interferometro specificato da T , oppure usano un **Algoritmo Greedy** per imitare il Ground Truth, e falsificare così gli esiti dell'esperienza.

In tutti i casi, i campioni di Borealis si comportano significativamente meglio di qualsiasi spoofer avendo un'entropia incrociata elevata rispetto al Ground Truth (Fig. 3.3).

3.3.3 Esecuzione dell'esperienza di campionamento con un numero elevato di fotoni e modalità

Vengono ripetute le misurazioni un'ultima volta considerando però un elevato numero di modi e fotoni, in cui il calcolo della probabilità anche di un singolo evento utilizzando un computer classico non sia fattibile.

In questo regime consideriamo media e varianza delle distribuzioni di probabilità del numero di fotoni di 216 modi e 10^6 campioni rispetto al ground truth e alle diverse distribuzioni realizzate dagli spoofer. E' bene osservare come i campioni ottenuti in questa dimostrazione siano generati dalla stessa famiglia di operazioni dei campioni generati nella precedente dimostrazione, in questo caso cambia solo la luminosità della luce compressa in ingresso. [24]

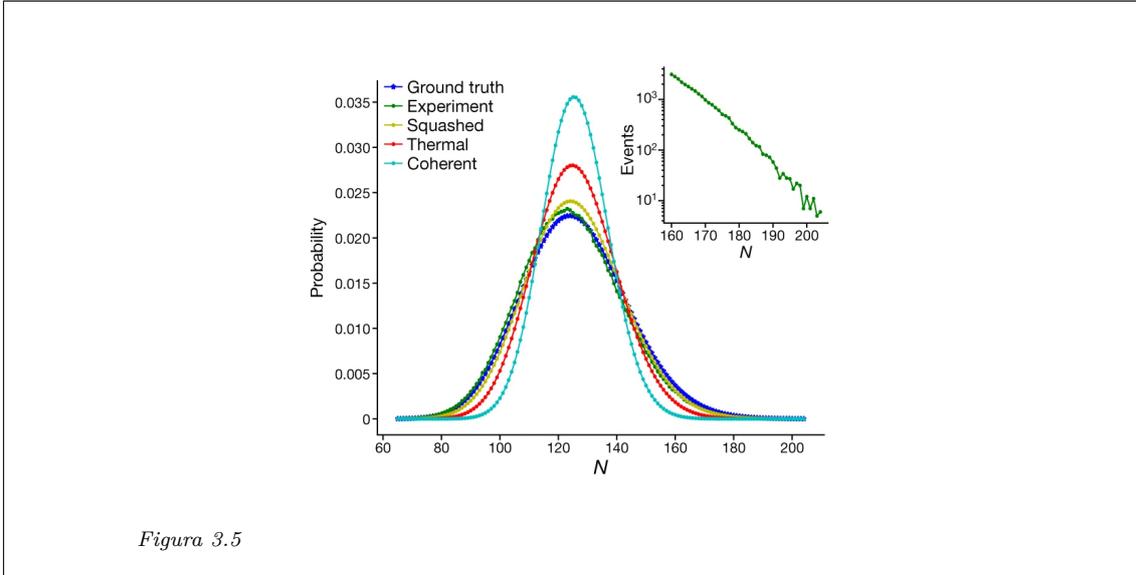


Figura 3.5

Figura 3.5: Distribuzioni totali di probabilità del numero di fotoni misurate nell'esperimento e calcolate attraverso il Ground Truth e da diversi spoofer.

Per costruzione, i campioni generati da ciascun avversario classico possiedono lo stesso numero medio di fotoni del ground truth e quindi centrato in $\bar{N}=125$, ciò garantisce agli spoofer condizioni eque per falsificare il nostro esperimento. [24] Tuttavia, è evidente come il valore della varianza degli spoofer sia diverso da quello del ground truth proposta da Borealis. [24]

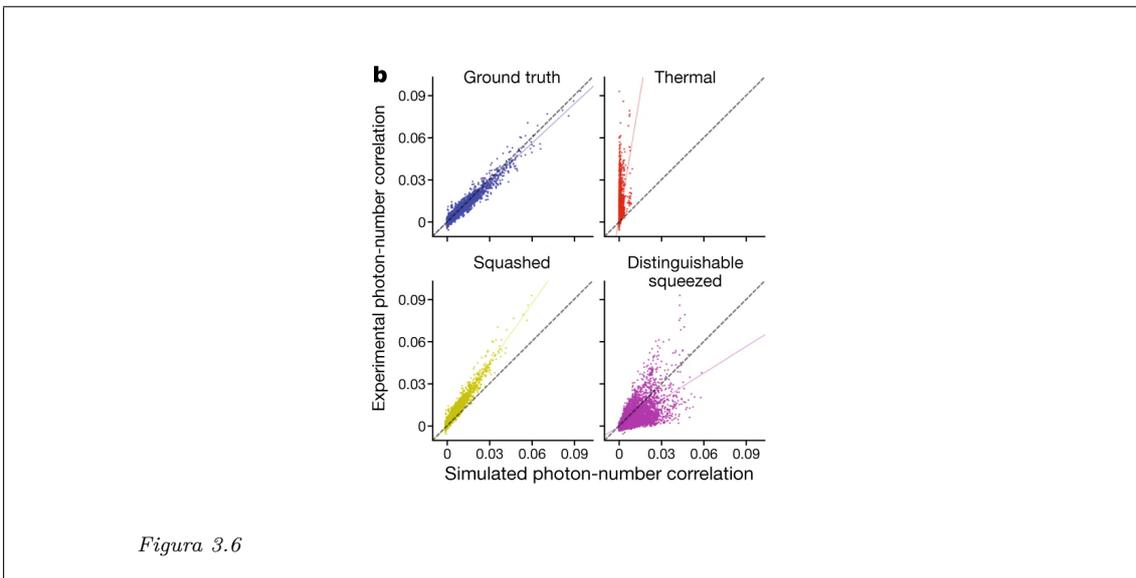


Figura 3.6

Figura 3.6: Distribuzioni totali di probabilità del numero di fotoni misurate nell'esperimento e calcolate attraverso il Ground Truth e da diversi spoofer.

Si noti inoltre come in questa dimostrazione ogni porta di ingresso dell'interferometro sia popolata con uno stato compresso. Questa proprietà indica che le descrizioni statistiche del terzo e quarto ordine del numero di fotoni sono estremamente piccole ($\approx 10^{-6}$).

Nella distribuzione di probabilità sperimentale del numero totale di fotoni, il risultato con la probabilità più alta è $\mathbf{N}=124,35\pm 0,02$ e la distribuzione ha un supporto significativo oltre i 160. Possiamo allora stimare il tempo necessario per simulare un particolare campione $\mathbf{S} = (\mathbf{n}_1, \dots, \mathbf{n}_m)$ con Fugaku, l'attuale supercomputer più potente del mondo, attraverso la seguente equazione:

$$\text{time}(N_c, \mathbf{G}) = \frac{1}{2} c_{\text{Fugaku}} M N_c^3 \mathbf{G}^{N_c/2} \quad (3.5)$$

Dove $\mathbf{G} = (\prod_{i=1}^M (\mathbf{n}_i + 1))^{1/N_c}$ rappresenta il parametro di collisione, in cui \mathbf{n}_i nella i -esima modalità, mentre N_c è il numero di distribuzioni rilevate diverse da zero. $c_{\text{Fugaku}} = c_{\text{niagara}}/128.8 \approx 4.41 \times 10^{-17}$ si riferisce alla velocità alla quale il supercomputer Fugaku può eseguire operazioni aritmetiche in virgola mobile, tipicamente misurato in termini di numero di operazioni in virgola mobile (addizioni, moltiplicazioni, ecc.) che possono essere eseguite per unità di tempo.

Infine, si considera $M=216$, anche se tale valore sovrastima leggermente il tempo impiegato da un sistema classico.

Sulla base di queste ipotesi si stima che, in media, Fugaku impiegherebbe 9.000 anni per generare un campione, o 9 miliardi di anni per il milione di campioni raccolti da Borealis. [24]

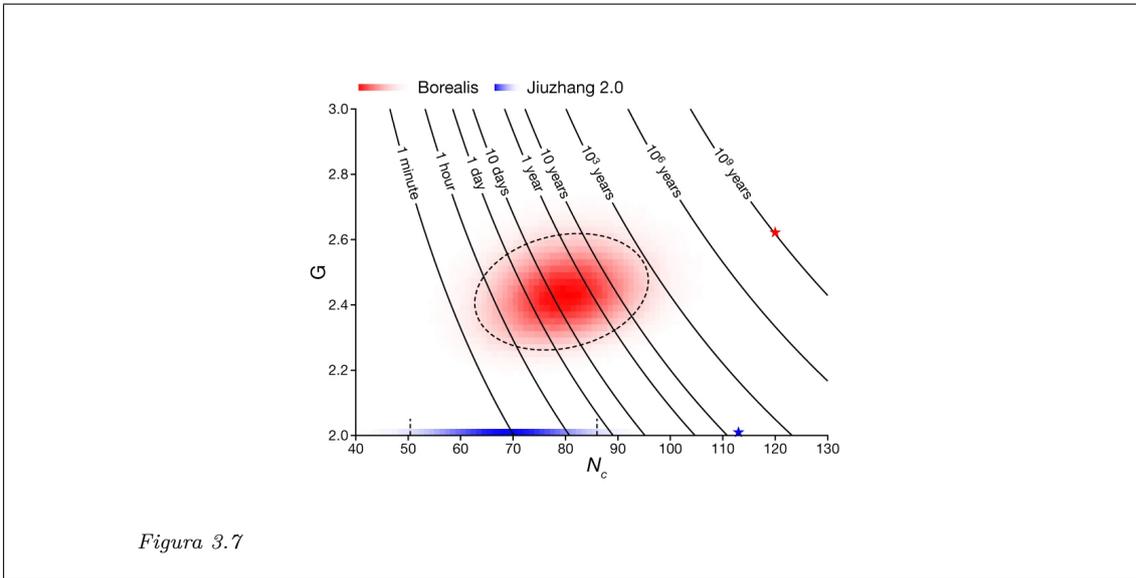


Figura 3.7: Distribuzione dei tempi di esecuzione classici di Fukagu per ciascun campione estratto nell'esperimento. Il campione con il tempo di esecuzione maggiore è indicato con una stella.

Per completezza all'interno del grafico sono stati inseriti anche i dati relativi l'esperimento di massima luminosità di Jiuzhang anche se il regime esplorato da Borealis è sette ordini di grandezza più difficile da simulare rispetto a quello di Jiuzhang.

3.4 raggiungimento del vantaggio quantico

E' stato dunque dimostrato con successo il raggiungimento del vantaggio quantistico attraverso GBS utilizzando una macchina che sfrutti il time domain multiplexing fotonico. A differenza dei precedenti dispositivi fotonici utilizzati per tali dimostrazioni, Borealis offre programmabilità dinamica su tutte le porte implementate, dimostra un vero rilevamento risolto in base al numero di fotoni e richiede un numero molto più modesto di componenti e percorsi ottici. Tra tutte le dimostrazioni del vantaggio computazionale quantistico, fotonico o meno, Borealis utilizza il maggior numero di sistemi quantistici indipendenti: 216 modalità compresse iniettate in un interferometro a 216 modalità con connettività tridimensionale, con un massimo di 219 fotoni rilevati. La dimostrazione è anche più resistente ai classici attacchi di spoofing rispetto a tutte le precedenti dimostrazioni fotoniche, rese possibili dall'elevato numero di fotoni e dall'efficienza del rilevamento implementata. Inoltre, l'uso riuscito di diversi loop in fibra stabilizzati in fase per fungere da memoria buffer efficace per le modalità quantistiche è una forte affermazione sulla fattibilità di questa tecnica, che è un requisito in molte architetture proposte per computer quantistici fotonici tolleranti agli errori. Questa dimostrazione segna quindi un progresso significativo nella tecnologia fotonica per il calcolo quantistico.

Conclusione

Con la seguente stesura si è voluto offrire una panoramica generale su come l'avanzamento delle tecnologie nell'ambito dell'informazione quantistica ne stiano sempre più confermando la supremazia rispetto ai principali sistemi classici. In particolare, è stata discussa una delle tecniche più promettenti per il raggiungimento del vantaggio computazionale quantistico, ovvero il Gaussian Boson Sampling, di cui come abbiamo visto ne è stata per la prima volta fornita una dimostrazione pratica utilizzando una macchina che sfrutti il time domain multiplexing fotonico.

Con Borealis, si apre finalmente lo spiraglio per la realizzazione di computer quantistici tolleranti agli errori, praticamente efficienti e che richiedano un numero molto più modesto di componenti e percorsi ottici.

Ciò rappresenta dunque una vera e propria pietra miliare nello sviluppo di questa tecnologia, permettendole di poter diventare una risorsa indispensabile per lo sviluppo sociale e tecnologico in quanto i computer quantistici possiedono le caratteristiche per il raggiungimento di complessità di calcolo mai esplorate fino ad ora.

In campo informatico ad esempio avrebbero la capacità di violare molti degli algoritmi utilizzati nella crittografia moderna, ma allo stesso modo avrebbero anche il potenziale per migliorare la sicurezza informatica sviluppando nuovi metodi di crittografia resistenti ai quanti. Potrebbero accelerare gli algoritmi di apprendimento automatico, consentendo un addestramento più rapido e un'analisi dei dati più efficiente, aiutando anche le attività di riconoscimento dei modelli, come il riconoscimento di immagini e parlato, fondamentali nel campo dell'intelligenza artificiale. Nel campo medico e chimico attraverso la simulazione di sistemi quantistici, consentendo ai ricercatori di studiare il comportamento di molecole, materiali e reazioni chimiche con una precisione senza precedenti, il che può accelerare notevolmente il processo di scoperta di farmaci prevedendo le proprietà e le interazioni di potenziali composti farmacologici. Sarebbero indispensabili nella progettazione di nuovi materiali con proprietà specifiche, come superconduttori o catalizzatori. D'altro canto il loro utilizzo potrebbe essere fondamentale anche in ambito finanziario per risolvere in modo efficiente problemi di ottimizzazione complessi, come l'ottimizzazione di supply chain, logistica o portafogli finanziari, avendo anche il potenziale per migliorare la modellazione finanziaria analizzando rapidamente grandi quantità di dati e ottimizzando le strategie di investimento, migliorando anche l'analisi del rischio e della gestione del portafoglio considerando una gamma più ampia di fattori e potenziali risultati. Sarebbero

estremamente utili anche in ambiti di uso comune, dato che riuscirebbero a fornire simulazioni più accurate e dettagliate dei modelli meteorologici e dei cambiamenti climatici, contribuendo allo sviluppo di modelli di previsione più precisi e consentendo migliori previsioni climatiche a lungo termine. In conclusione, i computer quantistici rappresentano la strada verso una nuova era di scoperte e rivoluzioni in uno svariato range di settori, ma come abbiamo visto la strada è ancora lunga complessa, e soprattutto sarà caratterizzata da moltissimi errori, errori indispensabili, perchè chi non commette errori, non ha mai esplorato nulla di nuovo.

Bibliografia e Sitografia

- [1] «"Why i called it 'Quantum Supremacy'»». In: (2019). URL: <https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/> (cit. a p. 2).
- [2] Andrew Hodges. *"Alan Turing The Enigma"*. Burnett Books, 1983 (cit. a p. 3).
- [3] «"Computer quantistico"». In: (2023). URL: https://it.wikipedia.org/wiki/Computer_quantistico (cit. a p. 3).
- [4] P.A.M. Dirac. *"The Principles of Quantum Mechanics"*. Clarendon Press., 1947 (cit. a p. 3).
- [5] Finesso Lorenzo. *"Lezioni di probabilità"*. Libreria Progetto Padova, 2019 (cit. a p. 3).
- [6] «"Elektroneninterferenzen an mehreren künstlich hergestellten Feinspalten"». In: (1960). URL: <https://doi.org/10.1007/BF01342460> (cit. a p. 4).
- [7] «"Electron interferometry with the Elmiskop 101 electron microscope"». In: (1974). URL: <https://iopscience.iop.org/article/10.1088/0022-3735/7/9/016> (cit. a p. 4).
- [8] «"Experiment and the foundations of quantum physics"». In: (1999). URL: <https://doi.org/10.1103/RevModPhys.71.S288> (cit. a p. 5).
- [9] «"Die gegenwärtige Situation in der Quantenmechanik"». In: (1935). URL: <https://doi.org/10.1007/BF01491891> (cit. a p. 5).
- [10] «"Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?"» In: (1935). URL: <https://doi.org/10.1103/PhysRev.47.777> (cit. a p. 6).
- [11] «"Imaging Bell-type nonlocal behavior"». In: (2019). URL: <https://www.science.org/doi/10.1126/sciadv.aaw2563> (cit. a p. 7).
- [12] Nielsen Michael A.; Chuang Isaac. *"Quantum Computation and Quantum Information"*. Cambridge University Press, 2010 (cit. a p. 8).
- [13] «"Quantum entanglement". Reviews of Modern Physics"». In: (2019). URL: <https://doi.org/10.1103/RevModPhys.81.865> (cit. a p. 8).
- [14] «"Ioni intrappolati per il futuro computer quantistico"». In: (2020). URL: <https://ilbolive.unipd.it/it/news/ioni-intrappolati-futuro-computer-quantistico> (cit. a p. 9).
- [15] «"Punto quantico"». In: (2023). URL: https://it.wikipedia.org/wiki/Punto_quantico (cit. a p. 9).

- [16] «"Importante scoperta di Microsoft per la realizzazione di qubit topologici"». In: (2022). URL: <https://www.quantumcomputinglab.cineca.it/2022/03/24/importante-scoperta-di-microsoft-per-la-realizzazione-di-qubit-topologici/> (cit. a p. 9).
- [17] «"Computazione quantistica con la risonanza magnetica nucleare"». In: (2022). URL: https://www.researchgate.net/publication/307588243_Computazione_quantistica_con_la_risonanza_magnetica_nucleare (cit. a p. 10).
- [18] «"Un qubit da un difetto del diamante"». In: (2015). URL: https://www.lescienze.it/news/2015/01/05/news/qubit_difetti_diamante-2430696/ (cit. a p. 10).
- [19] Carrol Sean. *"Dark Matter, Dark Energy: The dark side of the universe."* The Teaching Company, 2007 (cit. alle pp. 10, 11).
- [20] «"Efficient quantum memory for single-photon polarization qubits"». In: (2019). URL: <https://www.nature.com/articles/s41566-019-0368-8> (cit. a p. 12).
- [21] «"Quantum sampling problems, BosonSampling and quantum supremacy"». In: (2017). URL: <https://www.nature.com/articles/s41534-017-0018-2#Equ3> (cit. a p. 22).
- [22] «"The Computational Complexity of Linear Optics"». In: (2010). URL: <https://doi.org/10.48550/arXiv.1011.3245> (cit. a p. 22).
- [23] «"Gaussian Boson Sampling"». In: (2017). URL: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.119.170501> (cit. alle pp. 24, 27).
- [24] «"Quantum computational advantage with a programmable photonic processor"». In: (2022). URL: <https://www.nature.com/articles/s41586-022-04725-x> (cit. alle pp. 29–31, 33, 35, 37–39).
- [25] «"Toward large-scale fault-tolerant universal photonic quantum computing"». In: (2022). URL: <https://doi.org/10.1063/1.5100160> (cit. a p. 30).
- [26] «"2-D Cluster States for "One-Way" Quantum Computing"». In: (2019). URL: <https://www.optica-opn.org/home/newsroom/2019/october/2-d-cluster-states-for-one-way-quantum-computing/> (cit. a p. 32).

Elenco delle figure

1.1	Figura di interferenza con numero di elettroni progressivamente variabile.	5
1.2	Esperimento della doppia fenditura effettuato con elettroni singoli. . .	5
1.3	Immagine full frame che registra la violazione della disuguaglianza di Bell e implementa la scansione del cerchio di fase.	7
1.4	Rappresentazione di un qubit attraverso la sfera di Bloch	7
1.5	Modello standard delle particelle elementari	11
2.1	Rappresentazione schematica di un'istanza a 5 fotoni e 32 modalità del problema di Boson Sampling	21
3.1	Rappresentazione dei cluster states.	32
3.2	Circuito ottico che implementa Borealis.	33
3.3	Dati relativi all'esperimento appena proposto, con numero di fotoni N crescente da 3 a 6.	35
3.4	Confronto dei valori di entropia forniti dall'esperimento con quelli dei principali spoofer.	37
3.5	Distribuzioni totali di probabilità del numero di fotoni misurate nell'esperimento e calcolate attraverso il Ground Truth e da diversi spoofer.	38
3.6	Distribuzioni totali di probabilità del numero di fotoni misurate nell'esperimento e calcolate attraverso il Ground Truth e da diversi spoofer.	38
3.7	Distribuzione dei tempi di esecuzione classici di Fukagu per ciascun campione estratto nell'esperimento. Il campione con il tempo di esecuzione maggiore è indicato con una stella.	39